TACKLING THE BARRIERS TO ACHIEVING INFORMATION ASSURANCE

A.C. SIMMONS

Doctor of Philosophy *2017*

University of Wolverhampton
School of Mathematics and Computer Science

Title

Tackling the barriers to achieving Information Assurance

A thesis submitted in partial fulfilment of the requirements of the University of Wolverhampton for the degree of Doctor of Philosophy

Author *Andrea C. Simmons,* MA, FBCS CITP, CISM, CISSP, M.Inst.ISP, *Student Number 0923294*

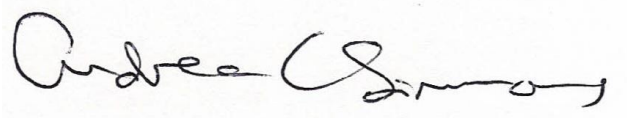
Supervisors Prof. Robert Moreton, University of Wolverhampton

Dr Martin Wright

Date December 2017

Authors Declaration

These are my own opinions, based on my own experiences and observations, but also my own prejudices.

Signature: 

Dated: .....7 December 2017.....

ABSTRACT

This original, reflective practitioner study researched whether professionalising IA could be successfully achieved, in line with the UK Cyber Security Strategy expectations. The context was an observed changing dominant narrative from IA to cybersecurity. The research provides a dialectical relationship with the past to improve IA understanding.

The Academic contribution: Using archival and survey data, the research traced the origins of the term IA and its practitioner usage, in the context of the increasing use of the neologism of cybersecurity, contributing to knowledge through historical research. Discourse analysis of predominantly UK government reports, policy direction, legislative and regulatory changes, reviewing texts to explore the functions served by specific constructions, mainly Information Security (Infosec) vs IA. The Researcher studied how accounts were linguistically constructed in terms of the descriptive, referential and rhetorical language used, and the function that serves. The results were captured in a chronological review of IA ontology.

The Practitioner contribution: Through an initial Participatory Action Research (PAR) public sector case study, the researcher sought to make sense of how the IA profession operates and how it was maturing. Data collection from self-professed IA practitioners provided empirical evidence. The researcher undertook evolutionary work analysing survey responses and developed theories from the analysis to answer the research questions. The researcher observed a need to implement a unified approach to Information Governance (IG) on a large organisation-wide scale. Using a constructivist grounded theory the researcher developed a new theoretical framework - **i3GRC™** (Integrated and Informed Information Governance, Risk, and Compliance) - based on what people actually say and do within the IA profession. **i3GRC™** supports the required Information Protection (IP) through maturation from IA to holistic IG. Again, using PAR, the theoretical framework was tested through a private sector case study, the resultant experience strengthening the bridge between academia and practitioners.

CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

A comprehensive list of Acronyms across the Information industry is available at

http://www.aiim.org/FAQs/Definition-of-Acronyms

Common Abbreviations

ALARM	The National Forum for Public Sector Risk Management
APMG	APM Group Ltd
AR	Action Research
BCS	Previously known as the British Computer Society, BCS now goes by its acronym only, reflecting more on the Chartered Institute for IT elements of the professionalism agenda http://www.bcs.org/
BERR	Department for Business Enterprise and Regulatory Reform (replaced by BIS)
BIS	Department for Business Innovation and Skills
BMIS	Business Model for Information Security
BoK	Body of Knowledge
BS	British Standards
BSI	British Standards Institution
BYOD	Bring Your Own Device
CBK	Common Body of Knowledge
CESG	HMG National Technical Authority for Information Assurance (*formerly*, Communications-Electronics Security Group) http://www.cesg.gov.uk/
CIO	Chief Information Officer
CISO	Chief InfoSec Officer
CMM	Capability Maturity Model
CNE	Computer Network Exploitation
CNSS	Committee on National Security Systems http://www.cnss.gov/
COBIT	Control Objectives for Information and Related Technology
COMPUSEC	Computer Security
COMSEC	Communications Security
COO	Chief Operations Officer
COSO	Committee of Sponsoring Organizations of the Treadway Commission http://www.coso.org
CPD	Continuous Professional Development
CPHC	Council of Professors and Heads of Computing
CPNI	Centre for the Protection of National Infrastructure http://www.cpni.gov.uk/ (formerly National Infrastructure Coordination Centre, NISCC)
CPS	Cyber Physical Systems
CQI	Chartered Quality Institute http://www.thecqi.org/
CSIA	UK Central Sponsor for Information Assurance

CSA	Cloud Security Alliance
CSA CSTAR	CSA Security Trust and Assurance Registry
CTAS	CESG Tailored Assurance Scheme
CyBoK	Cyber Security Body of Knowledge
DBIR	Data Breach Investigation Report
DHR	Data Handling Review
DoD	US Department of Defense, http://www.defense.gov/
DPA	Data Protection Act
DPF	Data Protection Forum
DHS	US Department of Homeland Security
DSO	Departmental Security Officer
DTI	Department of Trade and Industry (now BIS – Department for Business Innovation and Skills)
DWP	Department of Work and Pensions
EBA	European Banking Authority
EBK	Essential Body of Knowledge
ECJ	European Court of Justice
eGCF	e-Governance Competency Framework
ELCM	Enterprise Life Cycle Management
ENISA	European Network and InfoSec Agency http://www.enisa.europa.eu/
ERM	Enterprise Risk Management
EU	European Union
FIPS	Federal Information Processing Standards http://itl.nist.gov/fipspubs/
FISMA	Federal InfoSec Management Act
FSA	Financial Services Authority
GCHQ	Government Communication Headquarters
GDPR	General Data Protection Regulation
GPG	Good Practice Guide (CESG)
GCSx	Government Connect Secure eXtranet
GRC	Governance, Risk, and Compliance
GSE	Government Secure Extranet
GSi	Government Secure Intranet made up of (X.GSI, GSI, GSE, GSX, GCSX)
HIPAA	Health Insurance Portability and Accountability Act (US)
HMG	Her Majesty's Government (UK)
HMRC	Her Majesty's Revenue and Customs
HMSO	Her Majesty's Stationery Office
HR	Human Resources
i3GRC™	Integrated and Informed Information Governance, Risk, and Compliance
IA	Information Assurance
IA²	Information Assurance Architecture

IAAC	Information Assurance Advisory Council http://www.iaac.org.uk/
IAAF	Information Assurance Assessment Framework
IAB	Internet Activities Board
IAMM	Information Assurance Maturity Model
IAS	Information Assurance and Security
IAS#	CESG Information Assurance Standard by number (#)
IC	Internal Control
ICAEW	Institute of Chartered Accountants in England and Wales
ICO	Information Commissioners Office
ICT	Information and Communications Technology
IdA	Identity Assurance
IDS	Intrusion Detection Systems
IET	The Institution of Engineering and Technology
IG	Information Governance
IGE	Institute for Global Ethics
IIA	Institute of Internal Auditors
IISP	Institute of InfoSec Professionals https://www.iisp.org/
IM	Information Management
Intellect	The leading trade association which serves to represent its members in the UK technology industry and HMG
Info	Information
InfoSec	Information Security (general abbreviation; US sometimes used **InfoSec** to refer to *IS Security*)
InfoSoc	Information Society
InfoSy	Information Security (RAF abbreviation)
IO	Information Operations
IoD	Institute of Directors
IoT	Internet of Things
IP	Information Protection
IPCC	Independent Police Complaints Commission
IPS	Intrusion Prevention Systems
IRM	Information Risk Management
IRMS	Information and Records Management Society http://www.irms.org.uk/
IS	Information Systems
IS1	HMG InfoSec Standard No.1
IS3	HMG InfoSec Standard No.3
ISAB	InfoSec and Assurance Board
ISACA	Previously known as the IS Audit and Control Association, ISACA now goes by its acronym only, to reflect the broad range of IT governance professionals it serves. IS Audit and Control Association http://www.isaca-central.org.uk/
(ISC)²	Information System Security Certification Consortium

ISF	Information Security Forum
IS&A	InfoSec and Assurance
ISMS	InfoSec Management System
ISSA	IS Security Association http://www.issa-uk.org/
ISO	International Organization for Standardization http://www.iso.org/
IT	Information Technology
ITIL	IT Infrastructure Library
IT GRC	Information Technology Governance, Risk, and Compliance
ITSEC	IT Security
KPI	Key Performance Indicator
KTN	Knowledge Transfer Network https://ktn.innovateuk.org/
KYC	Know Your Customer
LGiU	Local Government Information Unit
MI5	Military Intelligence 5 (the Security Service)
MI6	Secret Intelligence Service (SIS)
MOD	Ministry of Defence
MPS	Manual of Protective Security
MSc	Master of Science
NAO	National Audit Office
NCC	The National Computing Centre
NHS	National Health Service
NHTCU	National Hi-Tech Crime Unit
N3	National Health Service Network
NISCC	National Infrastructure Security Coordination Centre
NIST	US National Institute of Standards and Technology http://www.nist.gov/
NSA	National Security Agency http://www.nsa.gov/
O-ISM3	Open Source InfoSec Maturity standard
OCEG	Open Compliance and Ethics Group
OCSIA	Office of Cyber Security and Information Assurance http://www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia
OECD	Organisation for Economic Co-operation and Development http://www.oecd.org/
OeE	Office of the e-Envoy
OMB	Office of Management and Budget http://www.whitehouse.gov/omb/
OSI	Open System Interconnection
OSS	Office of Strategic Services (US)
PACE	Pragmatic, Appropriate and Cost Effective
PAR	Participatory Action Research
PCI DSS	Payment Card Industry Data Security Standard
Per Comms	Personal Communications

PPT	People, Process and Technology
PSN	Public Sector Network
PwC	Pricewaterhouse Coopers
QA	Quality Assurance
RIMS	(the) Risk Management Society https://www.rims.org/Pages/Default.aspx
RMIAS	Reference Model for Information Assurance and Security
RTP	Risk Treatment Plan(s)
SDLC	Systems Development Lifecycle
SIRO	Senior Information Risk Owner
SOLACE	Society of Local Authority Chief Executives http://www.solace.org.uk/
SP	Special Publication
SPF	Security Policy Framework
SOA	Statement of Applicability
TED	Technology, Entertainment, Design http://www.ted.com/
TNA	The National Archives http://www.nationalarchives.gov.uk/
TOGAF	The Open Group Architecture Framework
UCF	Unified Compliance Framework
UCISA	Universities and Colleges IS Association http://www.ucisa.ac.uk/
UK	United Kingdom
UK CSIA	UK Central Sponsor for IA
USA	United States of America
US NSTISSI	US National Security Telecommunications and Information Systems Security Committee
USC	United States Code
WARP	Warning Advice and Reporting Point
WWW	World Wide Web
Y2K	Year 2000
X.GSI	CONFIDENTIAL Government Secure Intranet

ACKNOWLEDGEMENTS

I would like to thank all of my colleagues – both in the UK and beyond – for sharing their knowledge and experience in completing the survey that informed this dissertation. In particular, I would like to thank Andy Smith, for sharing his immense library of security related books – and equally for sharing his love of lifelong learning with me and with many in the InfoSec industry.

In addition I would also like to thank my Director of Studies, Professor Rob Moreton and my supervisor Dr Martin Wright for their consistent help and guidance on this voyage of academic discovery – but mostly for their patience!

I would like to acknowledge with warm gratitude both the unfailing support and tangible contribution of my beloved husband, Chris Simmons. Chris has endured long periods of solitude whilst I pounded the keyboard, and rewarded me with his precise and perceptive ear during the research stage – as well as providing a constant sounding board for thought structures, at all hours of day and night!

I would like to thank my father, Dudley Dolan, whose original suggestion was the main catalyst in me beginning this process seven years ago. I am grateful to him for my love of lifelong learning and to my mother, Jean Dolan, for the never waning ability to provide critical editorial oversight and terminological exactitude. Were it not for the Latin they were both so diligently taught in school, my fascination for the construction of sentences, the impact and the meaning of words, may not be so profound.

To my friends from whom this research endeavour has kept me, these past years, my thanks for your patience and tolerance. The time dimension of longitudinal research is brought home when you can chart it in terms of births (there have been several “in the circle”) and deaths (sadly there have been a few).

Finally, I would like to dedicate the outcome to my brother, Trevor Dolan [02/1966–02/2013], who did not live to see the end of it, nor manage to reach the same stage of his own difficult PhD experience. This one is for you, bro - rest in peace.

The person who speaks and writes precisely in a professional context is not being pedantic: she is being respectful of her interlocutors. She’s being a professional by thinking clearly about exactly what she means and then expressing herself as exactly as language will allow (Kabay, undated).

Part 1 – IA: Introduction, Literature Review, and Methodology

The Introduction provides context for the research area.

In the Literature Review, the fundamental principles of, and elements pertaining to, IA ontology is discussed in order to frame the professionalism discussion. The available different models for IA are evaluated.

The research strategy is discussed, the research paradigms are examined and the underlying ontological, epistemological, ethics and methodologies for IS research are selected. The aims, objectives and general assumptions are explained.

1 INTRODUCTION

1.1 Research Context

> *"There is nothing new under the sun, but there is something old we do not know."*
> *Ecclesiastes*

1.1.1 In 2009, the UK government set about an agenda to professionalise Information Assurance (IA) as observed in objective 4 from the UK Cyber Security Strategy: "building the cross-cutting knowledge, skills and capability to underpin all cybersecurity objectives" (UK Cabinet Office, 2011d). At the same time, UK Government policy shifted from reference to IA to reference to cybersecurity, in line with the prevailing dominant narrative (NAO, 2013, p.12). It is interesting to note that Russian narrative focuses on information space rather than cyberspace (Kingova, 2013). The UK vision was: "… for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values for liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society" (UK Cabinet Office, 2011d). In support of this endeavour, the UK Government released £650 million worth of funding to support the National Cyber Security Programme (ISM, 2010).

1.1.2 However, by March 2016, Government Communications Headquarters (GCHQ) provided commentary advising that despite spending nearly £1 billion on cybersecurity, the expected benefits had not been

realised (Gothard, 2016). A senior public sector IT chief was quoted in Computer Weekly as stating that:

> Security is an area of very significant challenge for government officials. We don't do security assurance in proportion to risk. There will be a rebellion soon because we can't get anything done (Hall, 2011a).

1.1.3 From the quote, it could be interpreted that industry overdoes security and that this hampers business progress. McClurg identified this phenomenon when he stated: "The norm for the 21st century security executive is protecting all the business assets all the time" (McClurg, 2005 cited in Dunkel, 2010). This situation often arises out of a lack of understanding of the application of effective risk management.

1.1.4 Year on year, through the Verizon findings (Verizon, 2006 - 2016), PricewaterhouseCoopers (PwC) surveys (running since 2000), Ponemon Institute research (Ponemon Institute LLC 2007, 2011-2014) and other research (Gillon *et al.*, 2011), the findings fluctuate between identifying that either those responsible are largely outsiders (hackers coming through networks or social engineering of employees) or insiders (disenfranchised employees). The latter correlates with social behaviour in recessionary times (op.cit.).

1.1.5 In 2016, Verizon conducted their tenth annual Data Breach Investigation Report (DBIR) (Verizon, 2017). In 2010, the DBIR (Verizon, 2011) showed that data loss through cyber-attacks had decreased sharply. However, by the end of 2014, the total number of breaches was higher than ever, where the losses of information were

experienced *both* electronically *and* physically, largely through human error (Verizon, 2015). In 2016, the greatest volume of breaches was perpetrated by outsiders (75 per cent). As a sector, whilst they were managing Capital Risk, the ramifications of the Global Financial Crisis of 2007-2008 continued to be experienced alongside ongoing data breaches. Research showed that the UK's major banks and lenders – including Barclays, HSBC, Lloyds Banking Group, NatWest, Nationwide, and Santander –reported multiple incidents to the ICO (Ashford, 2015; Vijayan, 2015).

1.1.6 These reports continually emphasised the need to remain vigilant in implementing and maintaining good IA practices. To do so, however, they need to understand the who, what, why and when of the required actions – which necessitates deeper understanding than sound bites from the news media. Stevens (2009) addressed this:

> We need to challenge our assumptions about what is expected of public authorities; about how we procure IT and from whom; about whether we should be collecting or sharing personal information at all. We need bold thinking, and those who do it need to know they will be supported if there are failures, not pilloried by the media and left out in the cold by their managers. It's innovation that will put an end to our data loss problems, and build a platform for 21st century information management.

1.1.7 2014 was a significant year for breach activity; 2015 was an equally active year with several companies suffering as a result of ethical standards failures. 2016 and 2017 saw increased ransomware

causing avoidable system harm. The belief that the private sector would "spontaneously generate the solutions needed for cybersecurity and minimize the need for government action" is proving to be misguided and lacking in evidence of success. Cyber insecurity (or lack of integrity and assurance) reflects what has been allowed, not just by omission, to grow. (Schneier, 2017).

1.1.8 Previously, a commonplace audit and post-breach or incident finding had been that employees (90 per cent) were a far greater threat to IA than outsiders (Kabay, 2002). However, most individuals are experiencing some form of information overload. The ongoing increase in breaches and the volume of data being extracted from organisations should not be occurring given the available mechanisms to protect the information. This reality has resulted in a significant increase in lawsuits which are targeting directors for their lack of application of duty of care by employing the available technological measures to adequately protect information (Mooney, 2015; Edwards, 2015; Schwartz, 2015).

1.1.9 None of this represents a new phenomenon. The first significant data breach publicly disclosed was in 1984 when the global credit information corporation known as TRW Inc. (now called Experian) was hacked and ninety million records were stolen. In 1986, sixteen million records were stolen from Revenue Canada. In a disappointing manifestation of the risk of being destined to repeat the same mistakes, in October 2015, there was another Experian related breach (Cunningham, 2015).

1.1.10 In June 2011, Microsoft published a paper regarding the difficulty of using the available statistics given that, in particular, "for rare phenomenon we are measuring a signal weaker than the noise in which it is embedded". Self-reported numbers may be used without screening for embellishment or exaggeration and this produces "estimates that cannot be relied upon" (Florencio and Herley, 2011, p.2). This is less of a phenomenon in the field of IA as those responsible for ensuring the protection of information assets are rarely likely to contribute to surveys honestly or accurately, irrespective of their purported anonymous nature. To do so, in and of itself, could result in an admission of a weakness that should never be exposed. Such conundrums are manifold in the area of focus for this research.

1.1.11 A key phrase, harnessed by the InfoSec practitioner and academic communities (Sasse, Lacey) during the preceding decade, particularly following on from the slew of data breaches in 2008 and 2009, was "human factors". "Human factors" have been an area of Information Systems (IS) research for many years, crossing the disciplines of economics, psychiatry, psychology, public policy, sociology, and anthropology and has been the subject of much academic research (Checkland, 1991). The Tavistock Institute made reference to the socio-technical inter-relationship in system design in 1949. Mumford and Beekman (1994, p.32) stressed that: "If a technical system is created at the expense of a social system, the results obtained will be sub-optimal". However, "human factors" had *not* been embedded in the practitioner realm of InfoSec nor IA until the early 21st century.

1.1.12 It is important to reflect on human nature as “this is a solid foundation for any practice of business management” of which InfoSec management is one. Thus, by default, so is IA (Stein, 2010, p.139). In the majority of the referenced material, IA specialists concur that security depends on people more than on technology (Ashenden, 2007; Blyth and Kovacich, 2001 and 2006; Collins, 1997; Glass, 1998; Virgo 2011).

1.1.13 The speed at which business, government, and citizens operate within the 21st century can result in context not always being understood by all participants and the resulting confusion can hamper the success of the required outcomes. Equally, the growth of IT, and the global and largely instant availability of information, as a result, has not necessarily made for a more intelligent, nor secure, human race (Stamper, 1973, p.1; Williams, 2014).

1.1.14 Both Lacey (2013a) and Schneier (2013b) held a discourse with regard to the long standing people, process and technology (PPT) triangle of operational expectation. Both believed that a rebalancing was required. Lacey argued that the IT security (ITSEC) world had become so complicated that we needed less in the way of people and process, and *more* technology. Schneier concurred that more technology was now required in order to address the volume of data created.

1.1.15 With regard to IP related roles, the task is invariably to provide reassurance as to the measures taken in order to apply known best practice for securing the information and for not reusing it beyond the

boundaries set by available legislation. However, reality dictates that there can be no such thing as 100 per cent security, nor can there be a 100 per cent risk-free situation (in any event). Thus it is unlikely that anyone can provide a 100 per cent degree of assurance with regard to their IP measures. Similarly, there are, no “free” internet products and services. The companies involved are seeking to turn a profit, to raise more funds, to please shareholders. They are generating revenue, usually at the expense of personal data, which can be seen to be a prized and valuable commodity (Best, 1996; Ashenden, 2007). For example, in April 2015 with the release of an age-guessing tool by Microsoft which went viral, the clear intention of the uptake was to gather geospatial data as well as personal metadata on each individual being deceived by the vanity of the appealing application (Vaas, 2015).

1.1.16 This context requires significant skill from the IA practitioners. IA must be maintained throughout the lifecycle of a system, as threats change with the shifting political or business environment, vulnerabilities appear and disappear. Thus, the configuration of the system changes and new weaknesses are discovered, and the impact of systems failure changes as dependency on a system develops.

1.1.17 The researcher contends that there has not been a compelling enough event to encourage sufficient adoption of the required practices, despite the increasing volumes of significant breaches. It is vital to appreciate the breadth of meaning for the term IA. As InfoSec is the forerunner for IA, without a depth of understanding of this terminology,

there is no foundation upon which to base communication and successful IA implementation, in neither the present nor the future. As Hutton (2008, p.17) wrote:

> IA is as much a problem of culture and human behaviour as it is a technical one. Without formal processes, procedures, audit and an overview of the situation, your information is vulnerable to organised crime, casual loss, and well-meaning staff who do not understand the risks associated with some of their current working practices.

1.2 Motivating Scenario and Problem Statement

> *"The enemy of knowledge is the illusion of knowledge."* Stephen Hawking

1.2.1 As a longstanding practitioner in the field, the researcher had been observing a lack of IA understanding that was inhibiting the collective ability of professionals across the public, private and third sectors and academia to adequately protect the information assets entrusted to them in order to ensure that they maintained the UK (and beyond) as a safe place in which to operate.

1.2.2 An article in the winter of 2008 highlighted research in the UK that claimed that 40 per cent of senior management respondents had little or no understanding of what the term IA actually meant (Hutton, 2008). This was after a number of years of work by various industry bodies to provide advice and guidance including the creation of a national strategy for IA. Senior management lack of understanding with regard to the constituent terminology has continued to be identified as an

issue of concern (Cornish *et al.*, 2011; Holtham, 2015). Thus, despite the launch of the first UK National IA Strategy (UK CSIA, 2003), revised in 2007 (UK Cabinet Office, 2007a), accompanied by clear direction to government departments from the Cabinet Secretary, there have been security breaches in all sectors, including significant breaches of the UK Data Protection Act during 2007 and 2008 (Burton, 2011).

1.2.3 Central government repeatedly articulated intentions for the UK to be the safest place to transact online (UK Cabinet Office, 2009b; UK Cabinet Office, 2011d; UK HMG, 2016b). However, the underlying implications are of flaws in the approach. This was further evidenced in subsequent research identifying that over 52 per cent of UK businesses were subject to a data breach in 2016 (Beaming, 2017).

1.2.4 This resonated with the researcher's own experience and motivated the commencement of research to investigate possible causes of the lack of IA understanding that appeared to be at the core of an inability to improve InfoSec and deliver the required Information Protection (IP), the ultimate outcome of IA activities. Note: IP is a term that will be used throughout this thesis to denote the overarching theme. IA and Information Governance (IG) are outcomes of successful achievement of IP. This level of abstraction, linguistic interpretation, and translation, is central to the research.

1.2.5 This research also analysed the likely success of the IA professionalism agenda in the context of the seven dimensions of professionalism (Brock, 2006), Lord Benson's nine obligations (1992)

and the work of Evans (2002, 2008) and Evetts (2003), but also in the context of an observed increasing shift in the dominant narrative to the perceived all-embracing term of cybersecurity, being adopted across all sectors at the sacrifice of IA.. In particular, the researcher was concerned that the term IA was at risk of being subsumed by the neologism of cybersecurity.

1.2.6 The research kept pace with the current government, its impact and progress as they pertain to IA. In May 2009, a change of UK government created an unstable and chaotic operational state, for the subsequent six months. There was a consequent change of political direction on the collection, processing, use, and sharing of personal data in ways that had been previously agreed upon. The result was a cessation of a number of cross-government IT related projects (Shanes, 2011). This was not wholly down to cost. The political dynamics had an impact on the direction of information management (IM) within the context of public sector governance. With the high volume outsourced usage of private sector companies for delivery of UK government public sector services, they were equally impacted.

1.2.7 There is an available body of literature regarding IA implementation, from both practitioners and academics. However, there appeared to be a collective amnesia regarding previous research, publications, available material relating to IA forming the basis of a successful cybersecurity protection framework (Cornish *et al.*, 2011, p.viii and p.30). The research sought to carry out a historical *analysis* reviewing the constituent parts, influences, and changes over time; then

undertaking *synthesis* evaluating whether IA remains fit for purpose; and finally providing a framework for future IA implementation.

1.2.8 As is often the case with longitudinal research, the objectives changed as a result of reflection on the findings and the available IA research; ongoing review of key publications and reports, shift in the dominant narrative, as well as a change in personal circumstances arising from undertaking a full-time global security policy and risk governance executive role in a large IT services provider between November 2011 and July 2015.

1.2.9 In the researchers' experience, for as much as the volume of available information has increased, the level of IA understanding has been decreasing. This has had a critical impact on the effectiveness of implementation of the specific and necessary requirements. The lack of IA understanding is potentially central to the cause of the skills crisis (Shah, 2013; ISACA, 2014; Millman, 2016). In February 2017, Sir Vince Cable discussed related history identifying low adoption of apprenticeships in the context of poor decisions taken with regard to educational standards, confirming that had been discussion about a skills crisis since shortly after the second world war (Cable, 2017).

1.2.10 The level of public confidence in the capacity and capability of all sectors (public, private, third) to protect their information remains diminished, reputations are tarnished and levels of trust remain low (Seldon, 2009). The researcher contended that lack of IA understanding was putting at risk the successful maturation of the UK information society (InfoSoc). If ignorance continues to prevail, IP will

not succeed which will damage not only the UK economy but risks the safety and security of many citizens worldwide.

1.2.11 The problem statement is thus: IA practitioners do not understand what the term IA means. This represents a barrier to effective IA implementation, inhibiting all sectors to adequately protect information assets in order to ensure maintenance of the UK (and beyond) as a safe place in which to transact online, in alignment with the UK Cyber Security Strategy.

1.3 Aims and Objectives of the Research

1.3.1 In implementation terms, IA theory has been largely based on the independent and individual views of practitioners, often channelled by the speech acts of either military or governmental channels but with no reference to source definitions in order to maintain consistency across organisational boundaries. The author sought to research whether professionalising IA could be successfully achieved, in line with the UK Cyber Security Strategy expectations, providing a dialectical relationship with the past to improve IA understanding.

1.3.2 The research aimed to tackle this wicked problem from a multiple of different angles, providing a solution from the **IG** space, rather than adding to the existing IA space. Key characteristics of wicked problems are that they straddle a number of disciplines, are difficult to define, are socially complex, involve changing behaviour, are often multi-causal and hardly ever sit conveniently within the responsibility of any one organisation (Rittel and Webber, 1973, p.161).

1.3.3 The purpose of this research was to evidence IA understanding, to provide a contribution to both the existing ontology and to the enhancement of practice in an attempt to identify improvements for the future (Remenyi, 2014, p.xii) and to improve policy making and professional practice, rather than to pursue political goals, per se (Hammersley and Atkinson, 2007, p.17). A guiding principle applied was that in order to comprehend the future, we must understand the past. [Note: This work is a study of the ontology of *IA* and its effective implementation, rather than *InfoSec*.]

1.3.4 The objectives were fourfold: i) to improve professional practice in IA and enhance the understanding of the subject area; ii) to evidence an extensive body of available material, much of which appeared to be unknown to many who claimed to be "security professionals" which did a great disservice to the professionalism agenda spearheaded by the UK's Communications-Electronics Security Group (CESG), and to the ability of the discipline to mature; iii) to provide empirical evidence as to the next stage of IP focus for security professionals, within the roadmap progression from IT Security, through InfoSec through IA to IG as portrayed in Figure 1 below, and therefore; and iv) to produce a framework for organisations to follow to achieve appropriate levels of holistic IG (i3GRC™).

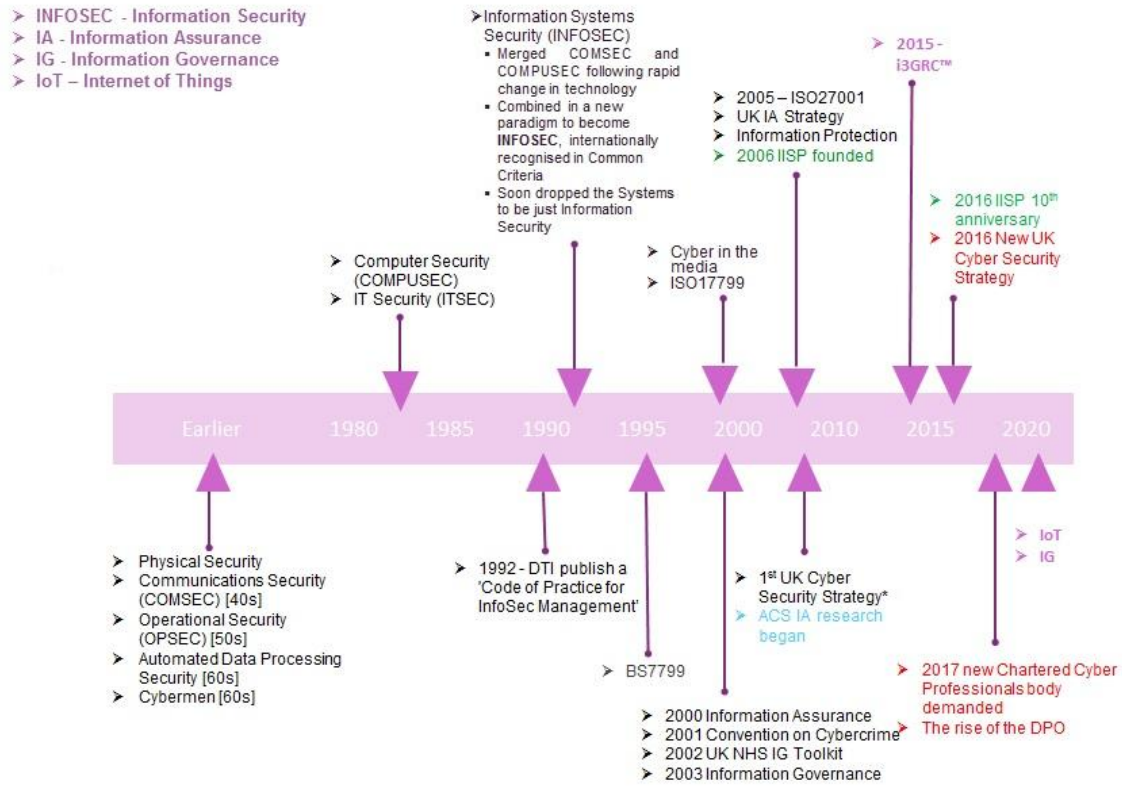


Figure 1: IT to IG Progression

1.4 Design and Structure of the Thesis

1.4.1 The thesis follows the research structure as outlined by Galliers and Land (1988) and is described Figure 2 below.

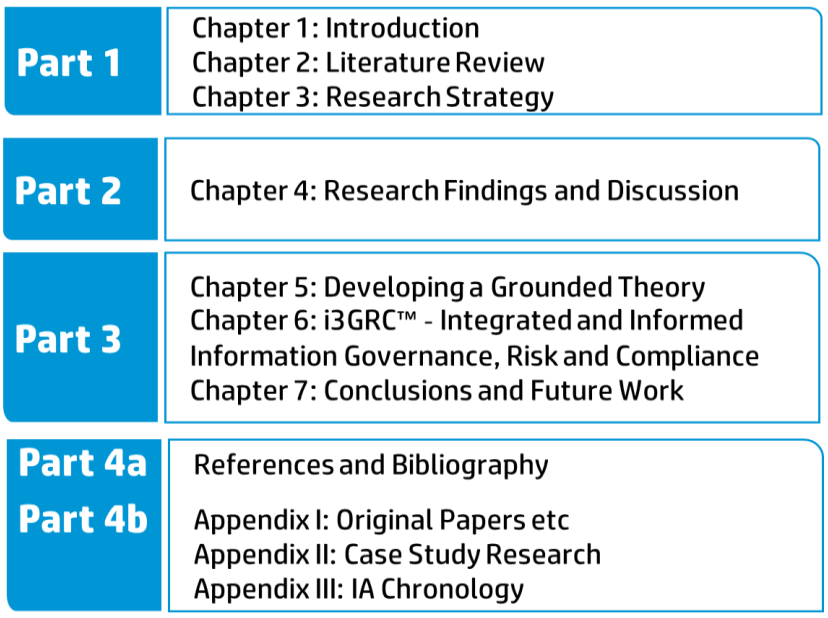


Figure 2: Thesis Structure

1.4.2 **Chapter 1: Introduction** addresses the context for this research.

1.4.3 **Chapter 2: Literature Review** sets out the main literature study of academic literature that underlies the rigour of the research and the political and business literature that confirms the relevance of the research topic. Relevant literature was brought into the discussions in the subsequent chapters as it related to the ongoing development of the Grounded Theory.

1.4.4 **Chapter 3: Research Strategy** provides a description of the methodology used to accomplish the research in this study, covering the research assumptions, paradigm and questions, discussing the purpose, methodology, and application of the respective methodologies.

1.4.5 **Chapter 4: Research Findings and Discussion** presents the findings and the supporting results analysis, providing outputs from the surveys, interviews and case studies. This chapter looks at the level of success of the research in demonstrating that IA has not been well understood to date. Discourse analysis identified the propagation of terminology utilised; the drivers and obligations experienced; the standards and measurements that drive compliance with regulation and legislation within the IA field; the impact of culture and politics on IA adoption and implementation, IA professionalism and aspects of the InfoSoc and how this has changed the breadth of IA requirements.

1.4.6 **Chapter 5: Developing a Grounded Theory** discusses the Participatory Action Research (PAR) case study findings which were

utilised to form a comparative, interpretative analysis to reach resulted in the formulation of a new Grounded Theory.

1.4.7 **Chapter 6: i3GRC™ Integrated and Informed Information Governance, Risk, and Compliance** presents a new framework following explanatory background as to the research progression that led to its creation. The findings from the previous Chapter contribute to the development of the framework.

1.4.8 **Chapter 7: Conclusions and Future Work** provides the research conclusions, reflecting on the research process and presents a number of areas of possible future work.

1.5 Summary of Research Approach and Methodology

1.5.1 The researcher used an iterative socially constructivist, inductive, design science research approach, in a critical realist ontology, with an interpretive epistemological paradigm. The research sought to answer the following questions: 1) can IA professional practice be improved through enhanced IA understanding?; 2) How has the extensive body of knowledge influenced professionals?; 3) Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec, through to IA?; and finally, 4) Is it possible to produce a framework suitable to support the route from IA to IG?

1.5.2 The methodology was mixed methods using interviews, surveys and PAR case studies, supported by historical research with a final output using Grounded Theory.

1.5.3 Choosing the appropriate research methodology is itself an area of constant academic debate, particularly when carried out in the context of business (Remenyi, 2014). The methodology used for the PAR case studies was ethnography by participant-observation in order to better understand both the public and private sector culture and dynamics and the impact of the various themes identified herein, the most important of which was the area of IA professionalisation.

1.5.4 Contextual and discourse analysis was undertaken, producing a set of non-hierarchical flat open codes around the themes of terminology, standards and measurements, culture and politics, and professionalism. The impact of the InfoSoc and the barriers to adoption were dealt with as secondary codes. Memos were continually recorded for each of these themes throughout the study and this write up is the collation and distillation of the work.

1.5.5 As the core topic was information based, the IS domain was a suitable multi-disciplinary base from which to provide a contribution to the study of IA; more particularly, in this case, within the context of the behavioural science and linguistics. A general structure for research in the field of IS in a business context involves: finding a suitable problem or research question; understanding what data is required to comprehend the issues involved; producing a data acquisition plan; accessing and managing the data; processing it appropriately; seeking more data if required; and finally interpreting the results. This approach has been confirmed as a valid methodology within the field of IS (Galliers, 1985; 1997).

1.5.6 The research was influenced by Critical Theory – how things *should* be, as distinct from Descriptive Theory – how things are; or Analytic Theory – why things are the way things are. This aspect of how things *should* be was fundamental to the outcomes of the Grounded Theory created through iterative and reflexive interpretation of the findings - *those involved in delivering IA, largely IT professionals by background, do not understand the scope of it and that leads to the need for the improvement framework* – Integrated and Informed Information Governance, Risk, and Compliance (i3GRC™). It was important for the researcher to produce a theory that fitted the real world, grounded in the empirical data (Gregory, 2011) that adds value to the role of the IA practitioner. In so doing, an appreciation of Design Science Research was realised.

1.6 Research Contribution

1.6.1 This practitioner research contributes to the learning of the discipline of IA, addressing a gap in knowledge through reviewing the available Body of Knowledge (BoK) addressing existing IA frameworks, but also extant literature, adding a detailed chronology of IA references through related reports, publications, government policy, regulation, legislation and industry contributions, showing growth and depth across a lengthy time span.

1.6.2 Through peer review and testing, the scale of this historical BoK has been confirmed to be new to many and should aid practitioner understanding, addressing multiple confusing mixtures of the concepts of IT security, InfoSec, cybersecurity, IA, and IG. Furthermore,

contextual analysis regarding the prevailing level of understanding and implementation of IA practices provides empirical evidence that whilst there are multiple definitions for IA, there are equally as many error prone interpretations utilisation of which are resulting in insecure system design and risk of data breach.

1.6.3 The research contributes to the literature on the ontology of IA by providing empirical evidence of the codification of its understanding. At the time of commencement of the study (2009), no such equivalent work existed. However, as is the risk with longitudinal research, a not dissimilar study has been undertaken by Cherdantseva and Hilton (2013a) into the specific distinctions between the two terms – InfoSec and IA. Richardson (2012) also carried out parallel research, to an extent, though it was more specifically focussed in the military and national security domains of the UK, with an emphasis on addressing the ability to assure air-gapped systems in the cyberspace domain.

1.6.4 Cherdantseva and Hilton (2013b) called for the creation of an up-to-date conceptual model of InfoSec and IA to reflect the current era. Whilst they followed up with the creation of their own Reference Model for IA and Security (RMIAS), the findings of this research took a different direction, showing that a framework incorporating the more broad space of IG is required, in order to embrace the growth and complexity of organisational demands.

1.6.5 Scott (2004, p.70) elucidated IA history through the US military lens:

> It is clear that significant events of past military warfare have shaped the current structure of military and civilian IA

> programs ... the entire evolutionary model demonstrates that the concept currently known as IA did, in fact, evolve from earlier forms of information and information systems security concepts during warfare.

1.6.6 Scott (Ibid. p.69) suggested areas of future research: "It would be beneficial to explore these later events to discover what specific changes have occurred. …..Further research could also focus on a closer analysis of the various government policies implemented over the period covered by the evolutionary process."

1.6.7 This research provides a coherent academic structure upon which to base IA practice. The impact of the contributions available will largely be experienced across the practitioner community through conference presentations, industry journal articles seeking to share the outcomes and consultancy engagements.

1.6.8 The InfoSec industry largely operates in vertical silos which do not integrate with the existing interdisciplinary areas of information science. IA remains a separate endeavour, not sufficiently embedded across organisational domains. As identified by Keen (1980, p.9): "Unless we build on each other's work, a field can never emerge, however good individual fragments may be". The findings contribute to other IP related models, bringing together a number of multi-disciplinary groups who at present risk talking over each other rather than being heard coherently – InfoSec, IA, Information Risk Management (IRM), Records and Information Management (RIM) and IG. These are different groups of learned colleagues with agendas

that are operated as if entirely separate and yet, an understanding of the depth and breadth of IP indicates that the goals are the same.

1.6.9 Using the reflections from the Literature Review, combined with the input from IA academics and practitioners, this research sought to address the boundary breaking aspect. Coalescence can be found under the IG discipline, and *not* solely from the perspective of technology, but with the three elements of PPT in balance. However, the evidence suggests a need to add a fourth leg, that of politics, both internal (organisational) and external.

1.6.10 This research presents a unique comparison of membership bodies as part of the analysis of the IA professionalism agenda – work that has not been undertaken elsewhere. The findings also extend IA research by introducing a graphical representation of a proposed future ontology for the achievement of robust IP - the i3GRC™ framework. This new meta framework within which to articulate IA – in the context of IG – provides a unique contribution to industry and academia as part of the maturation of IP for all sectors; to broaden, deepen and mature the BoK, supporting system design, development, enhancement and improvement, taking forward the discipline in an appropriate direction.

1.6.11 Twenty-three presentations of the material have been given during the course of this research [see **Appendix I**, **Section 10.2**] in addition to the publication of two books: one providing reference to best practice in InfoSec (December 2008) *Achieving Best Practice in Public Sector Information Security*, Ark Group Publishing, and a second entitled

Once more unto the Breach – Managing Information Security in an Uncertain World, ITGI Publishing, (2012). This was revised and republished in 2014.

1.6.12 This research proposes connections and patterns between sets of data and evidence within the constraints of both personal prejudices and experience. Pragmatically, using this interpretivist approach has allowed for a "significant contribution to both theory and improvement of practice" (Remenyi, 2014. p.xii).

1.6.13 A further aspect of the uniqueness of this research is that it is not technology led – a requirement identified by Sherwood *et al*. (2005, p.xviii) - although the researcher disagrees with reference to there being "few" books:

> …there is a growing concern that the technology that attracts so much investment from businesses is not delivering what it promises, and it is clear that the reason is that developments are led from a technical standpoint, not a business one. There are few books that address this issue, either for ICT generally or information systems security specifically.

1.7 Summary Research Conclusions

1.7.1 This research has addressed a gap in the extent of understanding of the full meaning of IA in the context of professionalising it. The gap between IS research and practice has been widely recognized and observed (Guangco, 2007, p.4). Enhancement of understanding can be facilitated through mechanisms such as industry publications, education, and attending conferences. IS researchers and

practitioners hold separate conferences with little cross participation and representation (Straub *et al*., 2005). As Guangco (2007, p.7) observed, "networking activities have been limited within the boundaries of each community, instead of facilitating an exchange". Success can only be measured if practitioners have time and interest to avail of these; combined with awareness of their existence alongside funding for professional membership bodies in order to have access to journals.

1.7.2 Critical to addressing the "skills crisis" is the requirement to ensure that there is an "informed" skill base. Reliance on seasoned practitioners has a limited lifespan. Search, recruitment and talent companies all need to be engaged in this upskilling, as do regulators and policy makers. Teaching fundamentals and principles so that cross-organisational individuals can tackle any presented problems. The Literature Review chronologically records the history of available ontology from InfoSec through to what has been published on IA, linking back to the UK Government Sector (and beyond) [See **Appendix III: IA Chronology**] in order to align professionalism of IA to address the skills crisis.

1.7.3 Adopting the i3GRC™ framework will assist in reducing the crisis, as will situational awareness across the UK and beyond. Other research has identified a rise in anti-intellectualism: "the dismissal of science, the arts, and humanities and their replacement by entertainment, self-righteousness, ignorance, and deliberate gullibility" (Williams, 2014). This needs to be tackled.

1.7.4 This research was designed to signpost the depth of the BoK in order to reduce claims of a lack of available mechanisms with which to tackle any aspect of IA (now continually, often erroneously, referred to as cybersecurity) and ensure that these can be relied upon to guide and shape the discipline and successful future of the IA profession.

1.7.5 The research identified a plethora of confusing descriptions, explanations, and terminology. The available literature has consistently outlined the steps to follow to secure information assets, from gaining executive level buy in to implementing policies and procedures and embarking on culture change programmes. Why the activities are repeated is a cultural phenomenon that should be addressed by social scientists, though Dekker (2011) discusses some of the reasons for the behaviour.

1.7.6 For the sake of future IP, stronger collaboration between academia and industry must address that there appears to be more that should be known than unknown. Reduction in expenditure on further research is required, rather policy makers and implementers need to support embedding identified IA best practices.

1.7.7 In 2011, the UK Government brought together a large group of participants with the intention of “Fighting Fraud Together” (UK HMG 2011b). Given how much fraud occurs through the compromise of existing systems and electronic infrastructures, the researcher believes that there are more participants required to join the group. Having a different organisation for each type of threat is difficult to manage in the long term. The same challenge faces the private

sector; more silos are created to address different threat vectors (Fisher, 2010). In 2011, further research undertaken by Cornish *et al.* (2011, p.28) in this area agreed:

> ....despite the perceived fragmentation it is to government that industry tends to turn for intelligence and information, particularly on high-level cybersecurity threats. This proposed architecture involves the government, but cannot be led by it. The nature of the problem is ingrained and systemic to the extent that a central authority can merely provide incentives to encourage a societal remedy but cannot mandate it. In simple terms, the £650 million allocated to cybersecurity (over four years) by the SDSR cannot 'fix' or 'secure' the critical national infrastructure, though it can help to catalyse greater attention to these issues within government.

1.7.8 As Simms (2011, p.26) wrote:

> The haste and brevity of the communications media du jour - texts and tweets – are no excuse for poor writing although they help to explain it. People have lost the habit of thinking about what they want to say before they write it down. So they shouldn't be surprised if their audience doesn't pay much attention to what they've said either.

2 LITERATURE REVIEW

2.1 Introduction

2.1.1 The first chapter highlighted the context within which this research was positioned – global experience of increasing information losses (data breaches) despite a myriad of available reports, frameworks, standards, legislation, regulation, and guidance. This Literature Review identifies key foundation blocks for IA in order to provide clarity to both its definition and meaning within the context of the prevailing BoK. It is supported by an extensive chronological compilation of research and analysis of accessible primary and secondary sources – published books, newspaper, magazine content, government reports, industry whitepapers, public and private sector reports and survey results - combined with a review of available relevant industry and popular literature, provided in **Appendix III: IA Chronology**.

2.1.2 Towards the end of the first decade of the 21st century, the rhetoric was dominated by the prefix *cyber*, as if it were a new concept. This Literature Review has found many resources dating further back, which reinforced the need for good IA to be embedded on an ongoing basis (IAAC, 2000a-d). The global IT industry referred to "hi-tech crime", before that e-crime, at a time when every initiative was afforded the opportunity of putting an "e" for *electronic* in front of it - prior to the adoption of the "cyber" label – but did not re-brand all related activities as "hi-tech crime prevention".

2.1.3 In 2013, the UK National Audit Office (NAO, 2013) represented this situation visually with a timeline showing how the UK Government had issued IA strategy documents from 2001 through to 2008 and then in 2009 changed the focus to issue the first UK Cyber Security Strategy. Davies (2010) wrote that what people appear to be hearing is "something, something, security, something, something, *cyber*, something, something, *advanced persistent threat*, something, something".

2.1.4 Tibbs *et al*. (2013) articulated the scope of the cyber challenge as an academic exercise appearing to repeat, though updating the work undertaken by the Foresight project (UK HMG (2003a) a decade previously. It is an international and boundary-less issue. In Tibbs *et al*. (op.cit.), there is no reference to IA whereas its place is recognised within the Cyber Primer produced for the UK Ministry of Defence (2013). Tibbs *et al*. (op.cit.) expanded on the depth of the challenge the UK Cyber Security Strategy was written to address.

2.1.5 In 2010, the UK Government changed from Labour to a Conservative and Liberal Democrat Coalition and, in so doing, renamed a great many departments. The links for many of the identified historical references were not, in all cases, transferred to the National Archives and thus, whilst a high volume of resources have been previously published, a number of them may be lost forever, squandering valuable history and risking the ability to reap the rewards of learning lessons.

2.1.6 This aspect of IRM is a challenge for many organisations in all sectors. It is for these reasons that a number of pertinent historical articles are referenced in the Bibliography.

2.1.7 The history of IA in the UK is embedded in the defence world. The work of Richardson (2012) was undertaken in the military domain focussing on national security, which is outside the scope of this more operational, business focussed research. However, the models created within his research are valuable and portable and will be referenced in the Findings discussion in *Chapter 4*. For context, the scope of IA presented in Figure 3 below provides a reference point, visualising the multiple layers of complexity.

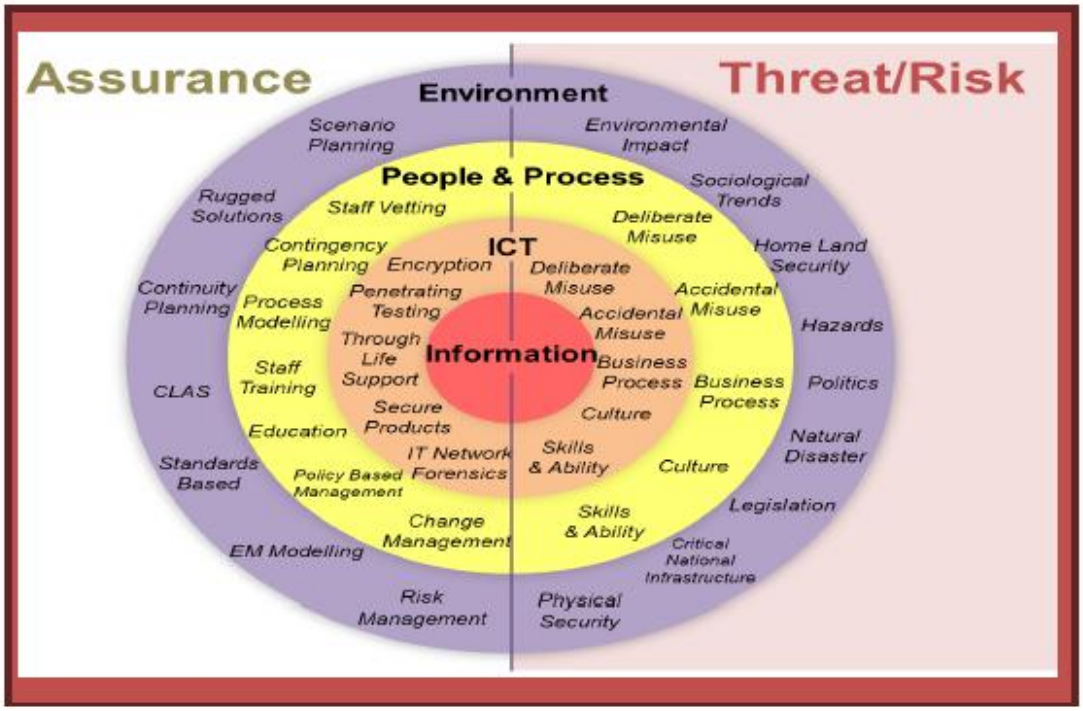


Figure 3: Assurance, Threat and Risk landscape, Source: Richardson (2012, p.100)

2.1.8 Dimopoulos (2007) thesis has IA in the title. However, its contents were almost exclusively focused on InfoSec and Risk Management, with nothing that explicitly embraced the terminology of IA. As an IA

resource, it is therefore thin and indicative of the continual evidence of authors using the term IA when InfoSec was what was being addressed. Cherdantseva and Hilton (2013a) took the decision to join the two together to form their Reference Model of IA and Security (RMIAS) discussed in more detail below. As identified by Cherdantseva and Hilton (2013b, p.9) "IAS means different things to different experts depending on their education and experience". Indeed, for some in the UK, IAS already stands for "**IA S**tandard" as produced by CESG (UK CESG, 2009 e/f/g/h, 2010a).

2.1.9 Despite there being more information easily accessible and available than in any previous generation, Cooper articulated that people are not reading enough; "books offer a great opportunity for managers to step away from the 'paced assembly line of managing' (Cooper, 2011, p.78). Blogging is an example of this too, where participants feel they have a voice but the results become noise in the maelstrom (Virgo, 2010; Room, 2009). This is not a new phenomenon (Toffler, 1970; Stewart, 2015) but one that will be visited throughout the Literature Review.

2.1.10 This Chapter defines IA and constrains the thinking and discourse to IA. Historically, sources have been largely focussed on *InfoSec*. In parallel with the timeline of this research study, a number of relevant *IA* focussed theses have been published (Cherdantseva and Hilton, 2014; Richardson, 2012) – which corroborated the need for attention to this discipline.

2.2 IA Origins

> *...That the further one looks back -- the further forward one can see...*
>
> *Winston Churchill, Quebec Conference, 1943*

2.2.1 The next section provides a chronological historical terminology review, in order to return to analyse IA adoption barriers. A full list of identified definitions is consolidated in **Appendix I, Section 10.20, Table 29: IA Definitions**.

2.2.2 From the United States (US), there is a history of iterations and development from Physical Security to Operational Security (OPSEC), Computer Security (COMPUSEC) and Communications Security (COMSEC). COMPUSEC tends to include database security; COMSEC tends to include network security and cryptography and is referred to by some as ITSEC. COMPUSEC and COMSEC were merged into InfoSec.

2.2.3 Kovacich (1998, p.2) stated that for his purposes, in writing about the role of the IS Security Officer, "the term *InfoSec*" incorporates the terms *information system security, information systems protection, information security, technology security, computer security, telecommunications security* and *technology protection"* – making this a comprehensive view. He added:

> The terms are all meant to describe the security and protection of the computers and telecommunication systems and the information that they store, process and transmit... [and

> InfoSec]... in any language, in any culture, in any country ...[is relative to the protection of those IS].

2.2.4 In 1999, InfoSec was defined in ISO/IEC 15408 as being "the protection of information against unauthorised disclosure, transfer or destruction, whether accidental or intentional" (IOS, 2009; Herrmann, 2003). Caplan and Sanders (1999) addressed the element of functionality within requirements as it related to InfoSec stating that functional requirements represent a statement of the security functionality or features a product is intended to provide.

2.2.5 In 2000, InfoSec came to be defined as:

> Protection of information systems against unauthorised access to or modification of information, whether in storage, processing or transit and against the denial of service to authorised users, including those measures necessary to detect, document and counter such threats (US NSTISSI 4009, 2000).

2.2.6 This was a natural progression from the earliest form of definition encompassing *confidentiality, integrity, and availability* (CIA) as the core elements of *InfoSec*. The model embraced the need to embed PPT as an overlay on the three main goals of security, that of achieving the CIA of the information you are seeking to protect. He articulated these in the manner of "Education, Training & Awareness (*people);* Policy and Practices (*process)* and *Technology"* (Ibid. p.4).

2.2.7 Parker (1981) explained the origins of the CIA triad, as represented in Figure 4.

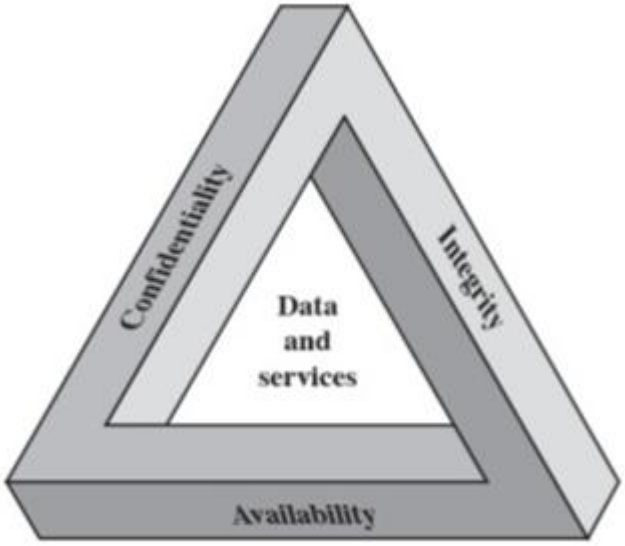


Figure 4: InfoSec Triad, Source: Gashi *et al*. (2015)

2.2.8 McCumber presented an original pedagogic framework for InfoSec, highlighting the constituent parts, including the need for a "common language/terminology in order to communicate effectively" (1991, p.4), shown in Figure 5 below.

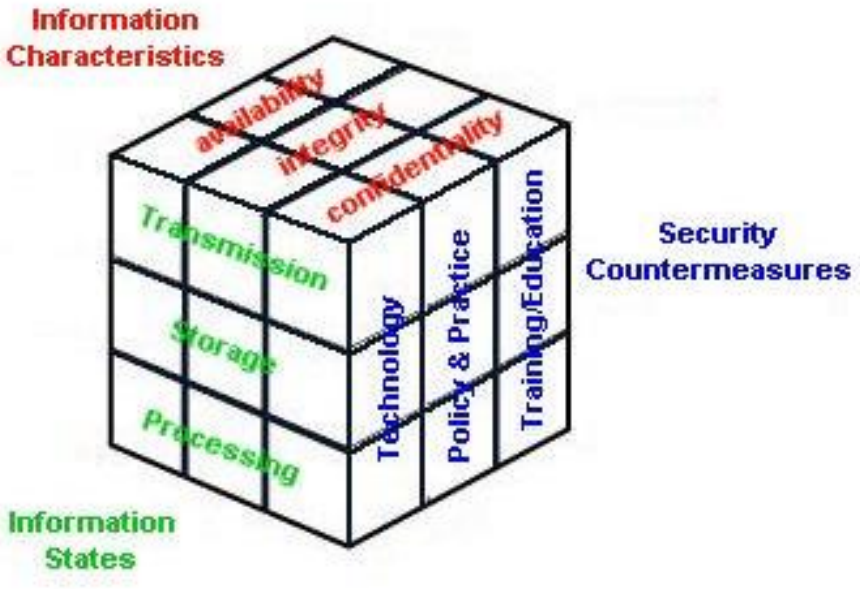


Figure 5: Original InfoSec Model, Source: McCumber (1991, p.4)

2.2.9 The most fulsome and concise definition of IA can be found in the US Department of Defence (DoD) (1998) *Joint Doctrine for Information Operations* (IO) (Joint Publication 3-13). It provided a broad focus of the information environment in which the Forces found themselves as a result of the continued scope of network communications, introducing two further terms to the CIA triad, those of *authentication* and *non-repudiation*.

> **Information Assurance.** Information operations that protect and defend information and information systems by ensuring their availability, integrity, ***authentication***, confidentiality, and ***non-repudiation***. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities. Also called IA.

2.2.10 **Confidentiality** covers protection against disclosure of information. **Integrity** is designed to ensure no unauthorised medication of data takes place. **Availability** is about the timely, reliable access to required data. **Non-repudiation** covers IP and identity through the delivery channels. **Authentication** is part of that proof of identity chain. These five key attributes are referred to more globally as the Five Pillars of IA (IWS, 2011). These pillars are supported by five common aims (Schou and Shoemaker, 2007, p.62): i) prevention; ii) detection; iii) containment; iv) deterrence and v) recovery. Mitigation, transference, and avoidance are often added to the list, as strategies for protecting information and reducing vulnerabilities.

2.2.11 Figure 6 below represents this scope definition.

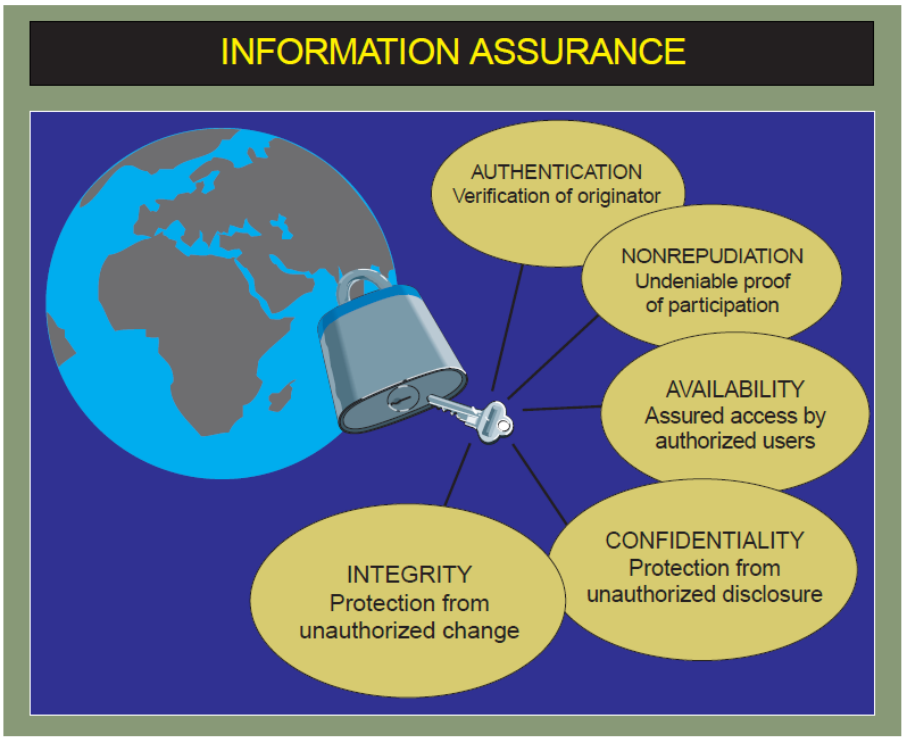


Figure 6: Joint Publication 3-13, Source: US DoD (1998, p.51)

2.2.12 The US Committee on National Security Systems (CNSS) on behalf of the US DoD produced a Position Paper on IA in April 1999 and referred to this definition. IA was articulated as taking a comprehensive view of the assurance responsibility "beyond establishing a top-level architecture, the IA concept does little more than integrate the conventional assurance activities of {COMPSEC} COMSEC, NETSEC, INFOSEC and security of operations into a single system" (Schou and Shoemaker, 2007, p.xxi and p.395).

2.2.13 Most other US DoD publications refer to the same definition (National Institute of Standards and Technology (NIST), CNSS, CNSSI etc.). A later Air Force Instruction bulletin (US DoD, 2001) identified that this definition could originally be found in U.S. DoD 3600-1 dated 1996

(source no longer available). McKnight (2002) also referred to this definition.

2.2.14 Research into the effective implementation of IA in the US DoD has been extensive – including, NDIA (1998) which identified best practices and Powell, Holmes and Pie (2010) who posited the IA Range. There have been a number of attempts to align IA with corporate strategy, thus elevating it above the domain of IT.

2.2.15 McCumber (Ibid.) showed how precluding other aspects of a full IA model (critical information characteristics, states, etc.) in security measures (policy) effectively restricts responses when it comes to dealing with threats that exist outside of the legal spectrum. The onus is on those involved in the implementation of policy to understand the environment within which they are operating and the likely factors that will impact on their success (Liles, 2011).

2.2.16 A decade later, there was an update to the *McCumber InfoSec Model,* positioning IA definition and direction for the future. The *Maconachy IA Model,* presented in a seminal conference paper, added the already defined information characteristics, *authentication,* and *non-repudiation*. Maconachy *et al.* (2001), working at the US National Security Agency at the time, saw IA as embracing the InfoSec CIA triad but needing to be articulated in terms of four dimensions: i) *Information States*; ii) *Security Services* (known as the Five Pillars); iii) *Security Countermeasures* (also known as controls or safeguards - embracing PPT aspects); and iv) *Time* (aligning with the Security Development Life Cycle (SDLC) as information is in constant flux

dependent upon time. Information can have a greater sensitivity depending on when it is produced or released). The model is represented in Figure 7 below.

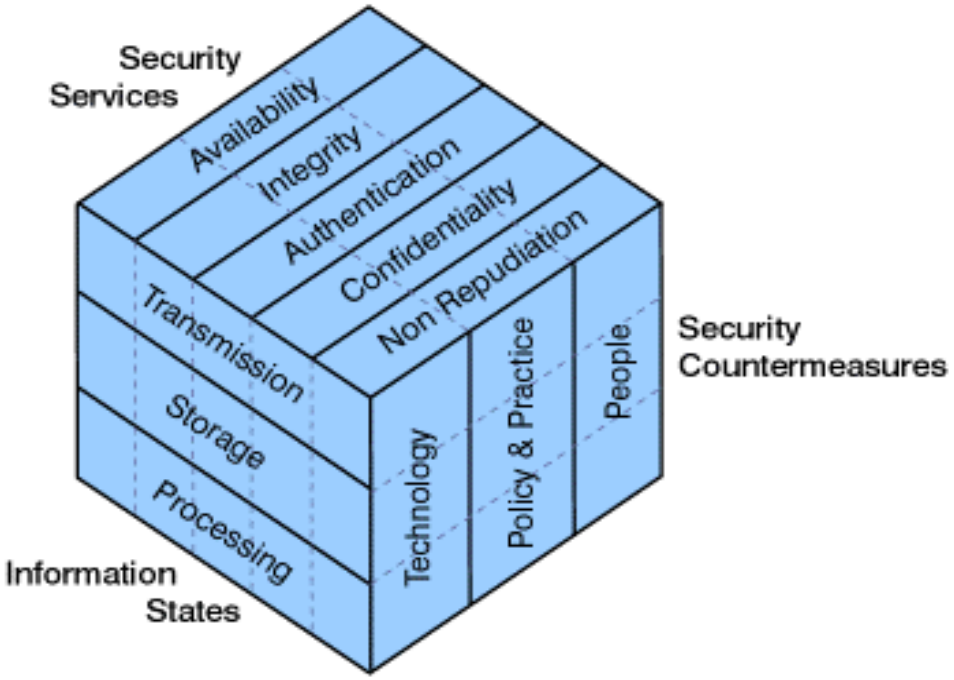


Figure 7: Maconachy IA Model, Source: Maconachy *et al.* (2001)

2.2.17 At the time of presentation, it was acknowledged that this was both a complex system description and a difficult concept to understand for non-professionals. This work sought to provide a scientific approach to explaining the development of IA, something that Shostack and Stewart (2008) missed in their understanding of what is already known and available within the BoK for IA when they called for definition expansion.

2.2.18 IA was born as system integration increased and, correspondingly, the need for security increased. Thus IA was intended to address proactive and reactive network defence; to encompass InfoSec and to broaden and deepen the profession. The integrated model was

designed to provide "a framework for questioning as well as teaching information assurance topics" (Ibid. p.309). The scope is represented in Figure 8 below.

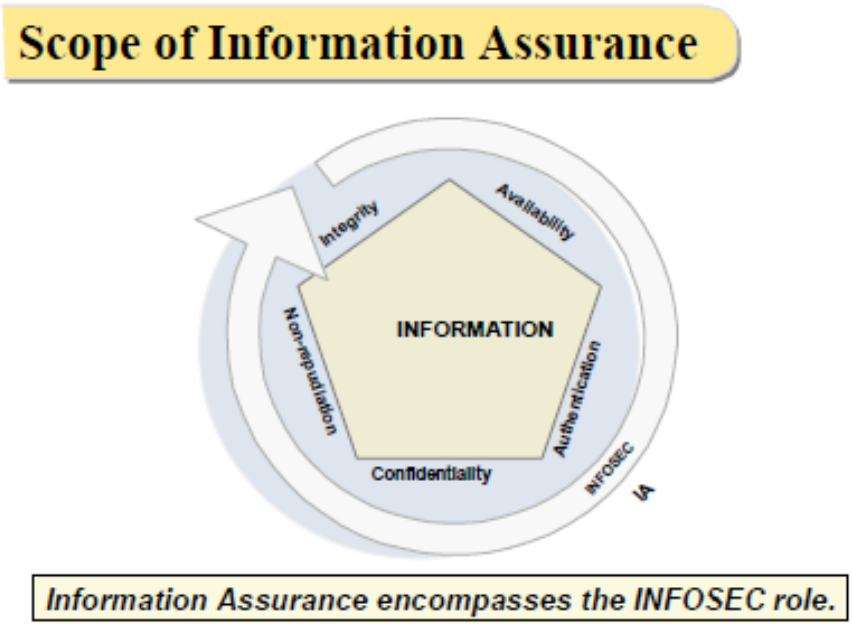


Figure 8: IA and InfoSec relationship, Source: Maconachy *et al.* (2001, p.307)

2.2.19 The Maconachy information states, previously articulated in the US National Security Telecommunications and Information Systems Security Committee publication NSTISSI No. 4011 (US NSTISSI, 1994), can be aligned with two specific UK Government approaches: i) Protective marking classifications in line with the Manual of Protective Security (MPS); and ii) Creating Profiles that correspond to levels of protection required for information (UK CESG, undated), which correspond with the likely countermeasures to be implemented in the solution space - (Being) Aware (*medium),* Deter (*medium high)*, Detect and Resist (*high)* and Defend (*very high)*. This was more recently updated to Prevent, Protect, Prepare and Pursue – a commonly

understood doctrine requiring a combination of Policies, Plans, Processes, and Doctrine.

2.2.20 Whilst the initial progression was from CompuSec to InfoSec, Parker (2011, per comms) disagreed with the ISO, NIST and the US DoD treatment of the elements, claiming that they are inconsistent. Parker saw that *confidentiality* and *integrity* referred to the secure state of information, whereas *authentication* and *non-repudiation* referred to controls to achieve CIA applied to people not information. He contended that the US DoD omitted *availability* from their list, leaving security defined incompletely.

2.2.21 Parker believed that "IA goes too far" given that it is an attempt to declare the intentions of an organisation to provide confidence, a pledge or a promise beyond protection from crime, abuse, misuse, errors and omissions "and doesn't seem appropriate". Parker considered the six elements described above (confidentiality, possession or control, integrity, authenticity, availability and, utility) to be attributes of information that are *atomic* in that they cannot be broken down any further; they are non-overlapping, referring to unique aspects of information. Information may have integrity but not be authentic and may be authentic (what the owner or custodian intended) but not have integrity (complete, whole and in good condition). Encrypted information may be available but without the key would not be useful.

2.2.22 Since 1998, the Parkerian Hexad (Figure 9 below) had been used as a model to explain his thinking.

Figure 9: Parkerian Hexad, Source: Parker (1998)

2.2.23 It can be argued that this is a contentious premise in the context of modern day business, where reputation is hard to gain and easy to lose if information is compromised as a result of a lack of implementation of available controls (op.cit.). Parker stressed that an important security element is protecting the *possession* of information whether it is confidential, or just proprietary and not confidential. Incorrectly defining integrity to include the *authenticity* of information is in conflict with most dictionaries. Parker used *authenticity* to refer to a state of information as opposed to how the US DoD referred to it – relating to people and access control.

2.2.24 Parker remained concerned that none of the available definitions include deception (op.cit.). Parker (2010) sought to express a more robust model for InfoSec, moving from the traditional (current) model (Figure 10) to a more modern view (Figure 11).

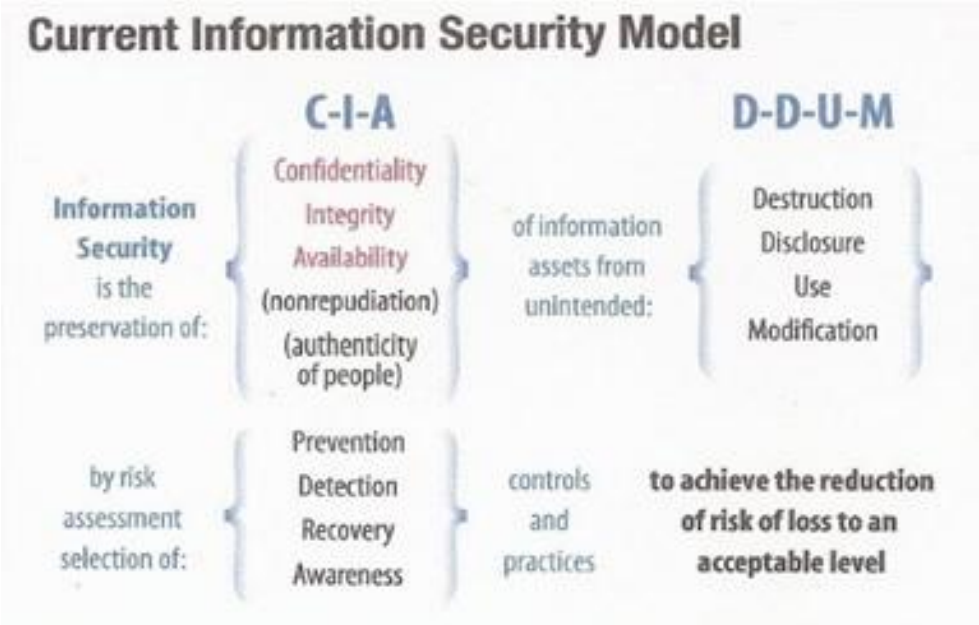


Figure 10: Current InfoSec Model, Source: Parker (2010)

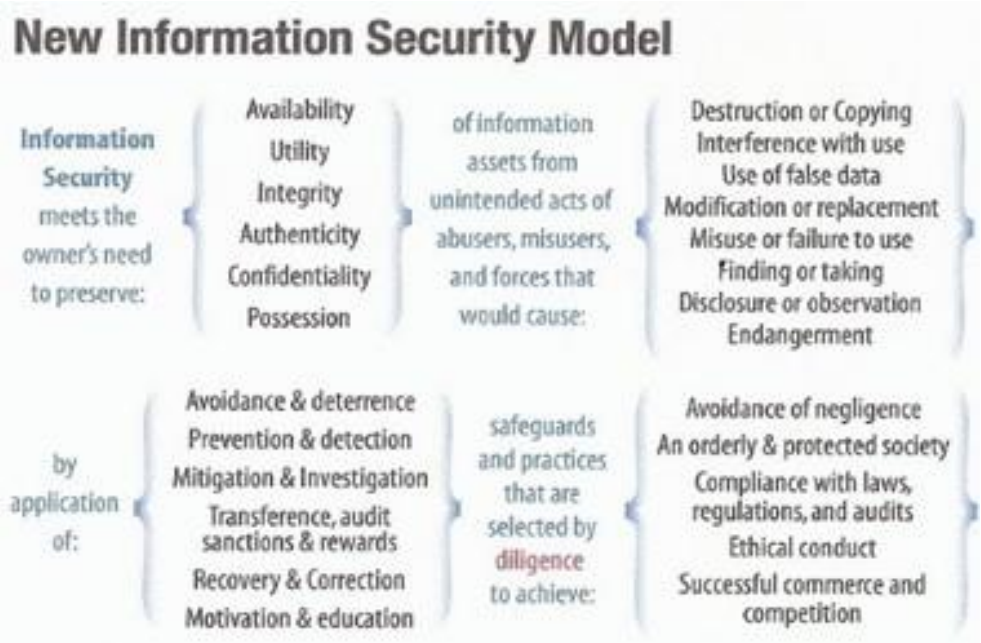


Figure 11: New Conceptual InfoSec Model, Source: Parker (2010)

2.2.25 This was inconsistent with the prevailing models with no correlation to either the McCumber Model or its Maconachy maturation in the suggested CIA improvement. The researcher questioned Parker directly on this and he went on to state that "Confidentiality and Integrity refer to the secure state of information, and Authentication and Non-Repudiation refer to controls to achieve CIA applied to people, not information" (op.cit.). Parker's views on definition appeared to be as prone to issues of subjectivity, confirmatory bias, and confusion around terminology, despite thirty years of writing about InfoSec and working in the industry, as any other contributor.

2.2.26 Herrmann (2002, p.8) proposed a broader definition of IA, whilst still using both terms (InfoSec and IA) relatively interchangeably:

> ...an engineering discipline that provides a comprehensive and systematic approach to ensuring that individual automated systems and dynamic combinations of automated systems and dynamic combinations of automated systems interact and provide their specified functionality, no more and no less, safely, reliably and securely in the intended operational environments.

2.2.27 Herrmann's contention was that using the term "automated systems" allowed for a broader scope than the use of the term "information systems". Herrmann (Ibid. p.9) saw IA as a three-dimensional challenge – encompassing "safety, reliability *and* security" - contending that a "safe, reliable and secure system by definition has proactively built-in error/fault/failure (whether accidental or intentional) prevention, detection, containment, and recovery mechanisms". This

book provides the basis for a clear understanding of IA for all practitioners, given the clarity it brings to the subject area.

2.2.28 Herrmann (loc.cit.) stated that "IA affects nearly all aspects of the everyday life of individuals and organisations. … IA has a pervasive role in today's technological society. This role can be divided into seven categories: i) human safety; ii) environmental safety; iii) property safety; iv) economic stability and security; v) social stability; vi) privacy, both individual and corporate; and vii) National security."

2.2.29 Schou and Trimmer (2004, p.i) identified that these dimensions also have states applicable to them – those of processing, storage, and transmission. These are the exact states that are a central focus of the Payment Card Industry Data Security Standard (PCI DSS), seeking to ensure that organisations focus on where their possession, usage, and exchange of credit card data is taking place.

2.2.30 Desman (2002, p.xvi) spoke of holding a particular philosophy with regard to InfoSec, that:

> ...it is not a technical issue, but a people issue. We simply use technical tools to resolve the problems we encounter. If we cannot speak and be understood, we will never reach our desired goals. As with the philosophy of democracy, if we do not gain the right to govern from those being governed, we will not. If we do not gain the cooperation of the rest of the company, nothing we do will come to fruition.

2.2.31 Effective InfoSec and IP is about supporting business processes "that provide[s] management with the processes needed to perform the fiduciary responsibility" rather than meeting security needs or audit requirements, per se. Barman (2002) also agreed with this within the context of security policy formulation, stating that the need is to identify what is to be protected in order to design appropriate security policies.

2.2.32 This was the discourse of the time, as Wylder (2004, p.21) pointed out:

> The effect of decentralization on the securing of corporate information assets is to force a change in viewpoint. The job of security, once regarded as a matter of data security, is now considered one of InfoSec, as the sum of the data elements is worth more than the individual parts. Databases now feed information to midrange machines and personal computers where there is additional processing performed. The job of the data security manager broadens to encompass all the data elements as they flow through the organization.

2.2.33 Wylder's writing was comprehensive with regard to the breadth and depth of InfoSec and what a professional should be doing in terms of their role. In contrast, the definitions provided by Schou and Trimmer (op.cit., p.i) were inconsistent with the findings of the Literature Review:

> *IA* contains all the elements of *InfoSec* (confidentiality) but also includes elements of availability, and integrity.... IA provides a view of protection that includes defensive measures in all three states -- processing, storage, and transmission. To defend

information and data there are three fundamental countermeasure categories: 1. Technology, 2. Operations, 3. Awareness, training and education.

2.2.34 IA contains all the elements of InfoSec – and yet Schou and Trimmer (Ibid.) presented only one – the C; and then say that it includes the A and the I as extras to make up the IA. The whole paragraph is linguistically challenging, confusing and unhelpful. A reader could absorb this and believe that InfoSec relies only on one attribute of CIA, and equally leave without understanding that IA has five core elements to it. This is another example of the importance of the need for accurate sentence construction to ensure clarity of meaning.

2.2.35 Dimitriadis (2011) contends that what we have ended up experiencing, in implementation terms, is a lack of consistency as each sector, industry, and organisation has appeared to implement security on the basis of their specific business needs and created a unique security definition to suit them. However, it could be seen that "InfoSec is no longer merely an emerging field of risk – it is well established as a critical and highly active field of risk that must be high on the agenda for every organisation's governing body" (Toomey, 2011, p.2).

2.2.36 Whilst there are many US NIST publications available, SP800-12 provides a robust discourse on the subject of *assurance* specifically in relation to IA, in particular, given that "*assurance is not an absolute guarantee that the measures work as intended*" (US NIST, 1995, p.103). This can undermine management and communication,

particularly when it comes to reassuring the public, whose personal information an organisation may be charged with protecting.

2.2.37 Figure 12 provides a visual representation of the distinction between InfoSec and IA:

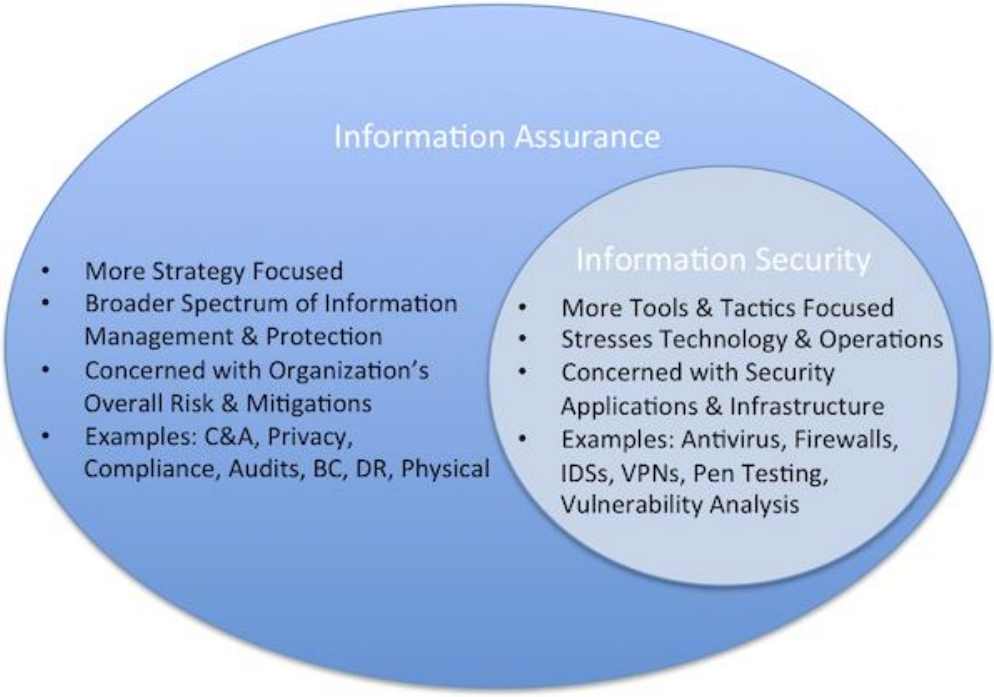


Figure 12: IA versus InfoSec, Source: Grec (2011)

2.2.38 Krause and Tipton (2004) only mention IA relative to software products (commercial or government "off the shelf") in relation to technical policy assurance, constraining the terminology rather than opening it up to the breadth of meaning it should have been afforded.

2.2.39 Numerous definitions of ***software assurance*** can be found. It is the level of confidence that software is free from vulnerabilities, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions as intended (US CNSS, 2003). The goal of *software assurance* is the ability to provide to software acquirers and users the justifiable confidence that

software will consistently exhibit its required properties, producing assurance as to the integrity, accuracy, and timeliness of the available information being produced. *Security* is what enables software to exhibit those properties even when the software comes under attack (IATAC, 2007). A high level of concern at the number of software vulnerabilities in critical infrastructures was highlighted in the US National Strategy to Secure Cyberspace, addressing the point that *known* vulnerabilities were going uncorrected and causing significant risk to the nation (US DHS, 2003).

2.2.40 It is essential to assure that the software within an asset base incorporates the required IA functionality. Schou and Shoemaker (2007, p.250) articulated that: "IA is linked to software because security functionality is enabled by it and software processes organizational information". Accreditation is a process allowing for formal acceptance of a system's security. There are frameworks available for achieving this, for example, **Common Criteria for Information Technology Security Evaluation**, with detailed explanations of assurance evaluation levels (Herrmann, 2003). CESG provides various accreditation schemes (UK CESG, undated, Certification). However, gaining assurance also highlights to an organisation the risks that must be accepted as part of business operations, either because it is not possible to address those risks or it is not economically feasible to do so. That focus enables the organisation to ensure that the risks remain, and will continue to remain within acceptable limits (Dowdall, Mattinson and Fagan, 2011).

Lack of commercial incentive for companies and lack of liability against software developers makes for more risky outcome – and a less professional one.

2.2.41 In order to be approved at any of the Assurance levels shown in Figure 13 below, platforms must be tested, such as Microsoft Windows, and a protection profile against which those tests are to be performed has to be agreed. For each level passed, Certification is received.

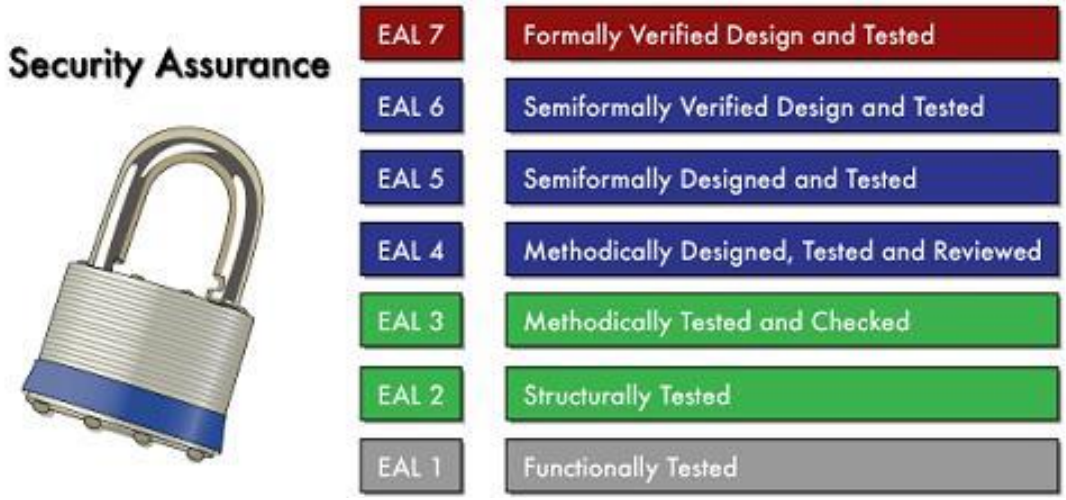


Figure 13: Software Assurance Evaluation Levels, Source: IT Compliance Institute (2010)

2.2.42 The State of the Art report provides a chronology of US focussed reports and research relating to *software assurance* (IATAC, 2007, p.3-5). The report references the genus of software security assurance work as far back as the 1970s. Evidence suggests that software development should be more secure. In 2013, research identified that "the average software developer, for example, doesn't own a single book on the subject of his or her work, and hasn't ever read one. That fact is horrifying for anyone concerned about the

quality of work in the field; for folks like us who write books, it is positively tragic" (DeMarco and Lister, 2013, p.11).

2.2.43 Bott (2005, p.19) takes the approach that "most software is not critical" and therefore, given the volume and propagation, it is too difficult to regulate software engineering for anything other than the most critical of systems – e.g. air traffic control. This argument seems weak. The basics of software engineering are not necessarily being learned by "script kiddies". This is overlaid with the complexity of having multiple vendor or product specific qualifications and certifications to be undertaken and maintained.

2.2.44 The inclusion of IA from a technical software perspective is depicted in Figure 14 below.

Figure 14: Software Assurance Universe, Source: US DHS (2010)

2.2.45 A description of the alignment between assurance and security can be found in an independent review of the security measures surrounding the UK Census 2011 (Dowdall, Mattinson and Fagan, 2011, p.29):

> The term “assurance” has a specific meaning within the security environment. Assurance is gained through activities confirming that the security measures that have been set in place are both effective and appropriate. It is not sufficient simply to set in place an assembly of technical and procedural controls; they must work, they must be seen to work, and they must be aligned to the underlying security problem. ... Assurance confirms that the security measures that have been put in place are aligned to the problems that they are intended to address, and that they can be relied upon to operate as expected.

2.2.46 There are different types of assurance – product, cryptographic, implementation, standards, operational and disposal. “The level of assurance required will depend on the security function that the system is performing” (Clarke, 2009). Satisfying *assurance* requirements provides confidence that the functional requirements have been met. The focus was more usually on *product* security, rather than overall *organisational* security.

2.2.47 There are multiple dimensions to the A in IA: i) Assurance that the processes and controls relied upon to manage risk and deliver performance are up to the task; ii) Assurance that the information relied upon to manage the business, set strategies, etc. are reliable; iii) Assurance on risk management provides the confidence to take risk; iv) Assurance that new projects, especially technology projects, will perform as desired; v) Assurance that IP and other assets are protected; vi) advisory services that contribute to the improvement of

governance, the management of risk, and controls; vii) Avoiding compliance disasters; viii) Reputation protection; ix) Improving sales and revenue performance through effective controls; and x) Direct cost-savings opportunities, such as from contract audits.

2.2.48 Delivering security per se does not increase profits; ergo it does not add value. However, there are growing instances where the ability to evidence assurance may add to profit margins, shareholder value and regulatory performance for year-end audits. The benefits can include the ability for businesses with audited accounts to borrow at lower interest rates, on the basis of the ability to evidence assurance that a product or industry standard is met and thus may increase sales, or may reduce insurance premiums (ACCA, 2010a/b/c).

2.2.49 Organization for Economic Co-operation and Development (OECD) Guidance states that the use of IS and networks should respect the legitimate rights and interests of others and "should be consistent with the values of a democratic society" particularly reflecting "the need for an open and free flow of information and basic concerns for personal privacy" (OECD, 1992, p.9).

2.2.50 In the UK, IA includes Data Protection and Privacy as a result of the close confidentiality links and OECD guidance requirements as implemented by IM and Quality, Records Management professionals and much more (Stahl, 2004). Rather than diminishing over time, this requirement has increased in importance in the passing two decades with the adoption of internet usage. The assurance function cannot be

successfully deployed until the risks are fully understood (Schou and Shoemaker, 2007, p.13).

2.2.51 Within industry, it is possible to choose from InfoSec, "information risk", Information Risk Management (IRM), IP or IA and also the US centric umbrella term of governance, risk and compliance (GRC) (TAAT, 2010c). GRC itself is prone to as many as twenty-two different definitions (Marks, 2011), although the most favoured is that provided by the Open Compliance and Ethics Group (OCEG, 2011).

2.2.52 Following research work at Forrester in 2002 (Rasmussen, 2015), OCEG was formed at the end of 2002 and began to discuss publicly, in various forums, the need for taking an integrated approach to GRC and internal controls (with consideration of culture) in 2003. OCEG used the acronym with the "C" representing Compliance because this was a siloed area of operations (each subject of compliance separate from the other) that needed great attention and harmonisation.

2.2.53 PwC had first used the term to represent a practice area of the firm. Others sometimes used the "C" to refer to Controls and some still do. In many ways, the C represents a C cubed, representing Compliance, Culture and Controls and GRC itself involves even more corporate systems (Quality, IT, Legal, Human Resources (HR) and others) but thirteen letter acronyms do not catch on (Racz *et al*., 2010).

2.2.54 The Information Technology (IT) industry is awash with duplicative acronym usage. For some, IA means **I**nternal **A**udit, *not* **I**nformation **A**ssurance. For others, IA stands for **I**dentity **A**ssurance or **I**nformation **A**rchitecture. IRM can mean **I**nformation **R**isk

Management or it could mean **I**nformation and **R**ecords **M**anagement. Team to team, department to department, in different organisations, the same acronyms can be used to mean different things. CI can mean *Configuration Item,* or *Continuous Improvement,* depending on team role in an organisation. There are many for whom the acronym CIA will signify the American **C**entral **I**ntelligence **A**gency, rather than the fundamental tenets of Information Security (InfoSec) – **C**onfidentiality, **I**ntegrity, and **A**vailability. The word "vulnerabilities" is another example of a speech act with multiple implications. There are *technical vulnerabilities* within code writing; there are *system design vulnerabilities*; there are *process and people vulnerabilities*. They each require different treatment responses: all are prone to vulnerabilities, but the context dictates the meaning and the understanding. These usage duplications add to confusion, misinterpretation and poor outcomes.

2.2.55 By 2004, GRC was well established based on the consultancy and audit work of PwC and OCEG use and was adopted across the advisory firms and key solution providers (Switzer, 2011). GRC is a lens through which an organisation can understand their business and appreciate why these elements need to work together in harmony (risk management and strategy), addressing fragmented processes, removing silos and working pan-organisationally. The international standard for risk management, ISO 31000 – articulated a framework requiring executive mandate and commitment, embedded risk management. The terminology in ISO Guide 73 - where risk is defined

as the effect of uncertainty on objectives - combines with ISO 31000 to provide a rounded understanding of the risk context (AIRMIC, Alarm and IRM, 2010, p.4).

2.2.56 Figure 15 below shows the confluence of areas.

Figure 15: Overall Assurance View

2.2.57 GRC is not about technology but about improved business processes. The difference experienced in an organisation *without* GRC (Figure 16) and *with* GRC (Figure 17) is depicted below.

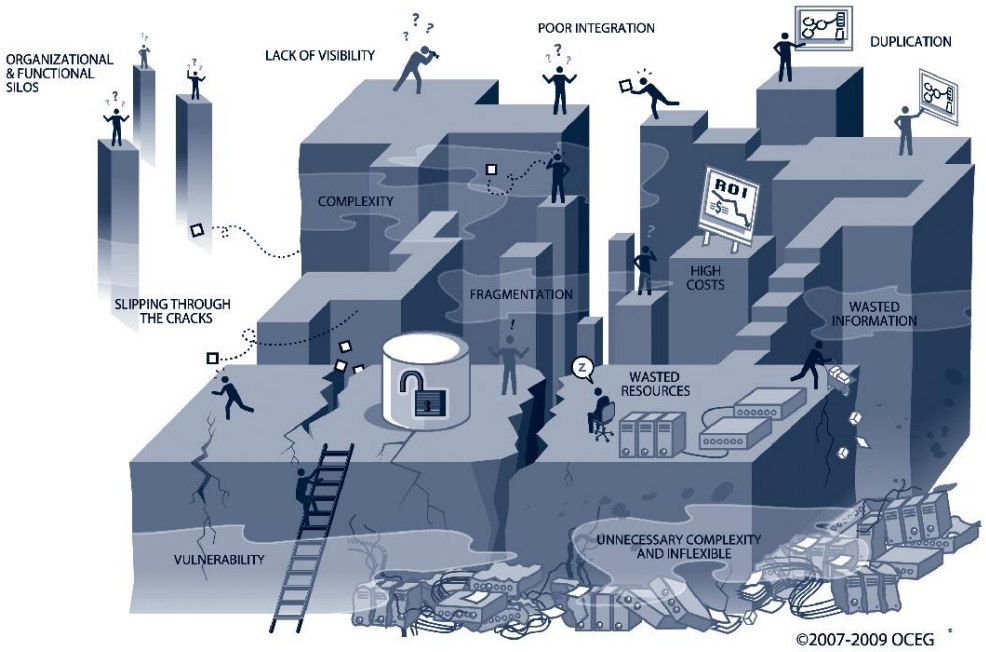


Figure 16: An Organisation without GRC, Source: OCEG (2009a)

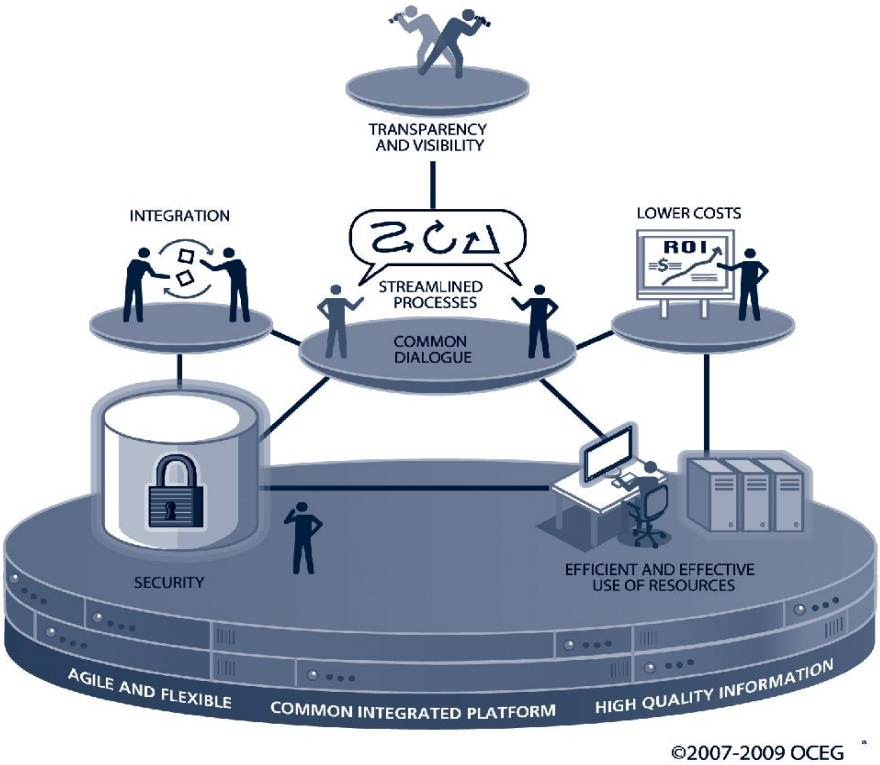


Figure 17: An Organisation with GRC, Source: OCEG (2009a)

2.2.58 Lacey (2009, p.198) was unimpressed with the use of the US term IA in the public sector. Lacey's reticence is from a position of not believing that it was possible for a security professional to encompass

the breadth of skills implied by the more wide ranging terminology – and an interesting perception that "the word 'assurance' also lacks the authority of 'security'" (loc.cit.). The public sector context remains slightly different: "Governments have different motivations for why they might spend on security. Sometimes the data is involved in national security ...other times, the obligation has to do with the mandatory nature of the data collection and the social contract that surrounds it" (Shostack and Stewart, 2008, p.108).

2.2.59 In the researcher's experience, this continues to miss the point and shows a lack of appreciation for the history of the development and growth of IT Security, through InfoSec to IA. In discussion, Tyrrell and Seddon (2014, p.31) addressed the sectoral differences in drivers asserting that "fear is pervasive in the public sector"; whereas in the private sector, the driving issue is profit. Further:

> ...the private sector (is) more amenable to improvement because effectiveness, eliminating waste and fulfilling the business's purposes are quickly measurable in the bottom line. But in the public sector fulfilling the purpose of the service effectively is way down the list of priorities – way below meeting targets and everyone keeping their jobs, even if their jobs are unnecessary.

2.2.60 Taylor *et al.* (2008, p.vii) – in the InfoSec Management Principles syllabus description document - begins by stating that "InfoSec ...is more accurately called IA" and then carry on throughout to use the terms inter changeably, which creates confusion and does a disservice to both strands of the profession. The definition does not

extend beyond the well-known CIA triad to include what this research has confirmed as being the already included IA elements of authentication and non-repudiation. Similar to the manual for the Certificate in InfoSec Management Principles, if the terms were so interchangeable then it should have been the Certificate in IA Principles in order to ameliorate future proofing as it would have reflected a more accurate understanding of the difference between the terms.

2.2.61 The evidence continued to show that IA is often used as a synonym for InfoSec (Boyce and Jennings, 2002). The issue of terminological difficulties within the security industry is not new (Schneier, 2003). Whilst it may be that "Attempts to create strictly defined vocabulary within InfoSec are likely doomed to failure as long as English remains a living language" (Shostack and Stewart, 2008, p.143); it is important to appreciate that practical responses flow from definitions. There is a natural cause and effect as a result of the speech acts and dominant narrative used.

2.2.62 In the late 1990s, the term IA was known only by small groups of InfoSec experts, often considered to be 'paranoid' or 'rigid' (Lacey, 2013b). Today, IA is well-known by a wider audience involved with UK public sector projects and private sector contracts ranging from high-level executives to engineers of many disciplines. Many have sought insight on IA processes through reading papers and attending briefings. Research undertaken by Tawileh and McIntosh (2007, p.6) appeared to use both InfoSec and IA interchangeably, causing

confusion to the outcomes; although the work did identify the need to embed the requirements across the whole business environment and the historical evidence that exists reflecting this need.

2.2.63 In the late 2000s, the status quo was similar, with only a small number of professionals truly understanding the breadth of meaning and the scale of available material upon from which to draw experience and wisdom (Hutton, 2008). In 2009, UK Government policy shifted to reference cybersecurity in line with the dominant narrative (NAO, 2013, p.12).

2.2.64 In the context of cybersecurity, there is a lack of evidence of any new principles. Tibbs (2013, p.112) identified this need:

> [in order] to understand and tame the Global Cyber Game ...[it will be necessary]...to establish a set of principles grounded in the root characteristics of information and power. These principles can then form design criteria for the development of cyber policy and strategy.

2.2.65 Excessive use of computer jargon and acronyms was identified as an issue with particular regard to user interface and system design (Galitz, 2007) and, separately, as an issue with regard to delivering InfoSec user awareness programmes (Peltier, 2005). As referenced in Goodell (1996, p.14), “How do you know when something new is coming? You know it when the language...is ugly. You cannot tell what these things are....”. There have been different examples of the progression of language, not all of which have merit. 2015 saw the entrance of ESRM – Enterprise Security and Risk Management - and

the term "phigital" – where the physical and the digital collide. Acronyms are often used within the written word in order to reduce repetition of cumbersome word strings. However, verbal abbreviation of common terms – where they are not so common; use of vernacular, industry speak, speed, shorthand, Twitter – are all creating misunderstandings between teams where extensive periods of time are required in explanation, building up animosity between departments because nobody appreciates being corrected (Simms, 2011, p.26). If an acronym has not been spelt out, a new term explained and the parameters from which the dialogue is to take place outlined, it will not matter how many times they are repeated, there will be different interpretation.

2.3 The Importance of Definition

2.3.1 In 2008, a survey highlighted that "40 per cent of senior management respondents had little or no understanding of what the term information assurance actually meant". The article reporting the survey went on to state that:

> Most organisations lack clear accountability for information assurance. With no single owner and usually so many well-meaning stakeholders, IA remains someone else's problem as a data-loss scandal, a collapse in customer confidence or negative press washes over your company (Hutton, 2008).

2.3.2 The researcher found this to still be the case, given the lack of understanding of the terminology and the expectation that the solutions remain the responsibility of IT professionals to address

(Holtham, 2015, p.13). Richardson (2012, p.18) identified that "the current structure of Assurance is both restrictive and intolerant to the problems it needs to define, explore and resolve". Richardson (Ibid. p.195) went on to provide his own definition of IA specific for the area of research – the military and national security theatre:

> IA is the assumed responsibility (Corporate Governance) and accreditation of a socio-technical Enterprise across the 5-layers of the Cyber Domain (Geographical, Physical, Logical, Persona and Cyber Persona), inclusive of their Business Processes, Information Operations, Information Exploitation, Management, Services, Technologies and Infrastructures. The socio-technical Enterprise is assured by appropriate levels of maturity and awareness within the 8-Dimensions of IA (Structure, Resilience, Dependability, Safety, Security, Protection, Trust and Risk Management).

2.3.3 These are eight *different* elements to those selected by Cherdantseva and Hilton (2013a) for their concept of the ***IAS-octave***: Confidentiality, Integrity, Availability, Accountability, Non-repudiation, Auditability, Authenticity, and Trustworthiness and Privacy within their ***Reference Model for IA and Security*** (**RMIAS**). The IAS-octave seeks to replace the CIA-triad, the McCumber Cube, and the Maconachy IA Model, detailing a comprehensive set of security goals (Cherdantseva and Hilton, 2013b). This is referenced as evidence of multiple overlapping models. The researcher contends that this academic duplication adds layers of complexity, rather than simplifying the

challenge of achieving IP in all domains. Risk management is an inherent element of InfoSec. Physical security has long been an understood requirement; convergence in these overlapping industries has been actively sought for some time. The issues are interwoven, not separately dependent. Since 1998, Purdue University has had CERIAS – the Centre for Education and Research in IA and Security (IAS) - so the concepts are not new.

2.3.4 There is an existing model - the Open Group (2011) InfoSec Management Maturity Model (**O-ISM3**) - that does not appear to have been considered within the work of Cherdantseva and Hilton (2013b, 2014). This model already identified CIA as an insufficient model for the security needs of the 21st century. The model mapped ISO 9001 quality management principles to InfoSec management systems. The latest version, dated 2013, also mapped to ISO 27001. The whole model focuses on common processes rather than on controls, processes which are shared across many organisations. Cherdantseva (2014) also reviewed the work of Von Solms (2001) and sought to enhance the multi-dimensional view of the InfoSec domain, to which the researcher has added italicised commentary: i) the Strategic/Corporate Governance Dimension; all subsequent standards and frameworks have sought to address this, COBiT, BMIS, ISO 27001 etc and yet still there is a need to explain to leadership the importance of the domain and the need for inclusion; ii) the Governance/Organisational Dimension; this would have, by default, included the Physical Security dimension and the Business Continuity

Dimension – by creating multiple vertical silos, the industry continues to create duplication of effort and complexity; iii) the Policy Dimension; iv) the Best Practice Dimension; v) the Ethical Dimension; vi) the Certification Dimension; vii) the Legal Dimension; - by default this must contain the Privacy Dimension, given the requirement to comply with relevant legislation with regard to the protection of personally identifiable information (PII); viii) the Insurance Dimension; - this should be part of the Governance/Organisational Dimension – it is a part of doing business, a management decision; ix) the Personnel/Human Dimension; ix) the Awareness Dimension; the researcher wonders why this is not part of the Personnel/Human Dimension – who else is going to be being made aware?; xi) the Technical Dimension - this must, by default, contain both the System Development Dimension which ensures that the security is built into the development process; and the Security Architecture Dimension; it appears to be a constant failing of the collective IT industry that "Security" has been treated as a separate vertical organisational activity rather than an intrinsically horizontal one; xii) the Measurement/Metrics (Compliance monitoring/Real time IT audit) Dimension; and xii) the Audit Dimension. This list is consistent with the regular industry approach of separating out activities, rather than bringing them together and ensuring a broader understanding of more issues with less duplication of effort. The researcher believes this adds misunderstanding to an already confused domain. Significant difference in focus in the last twenty years can be seen in the

Compliance space. Regulation, standards, policies and contracts are variations of the compliance requirement which could create a new Dimension: xiv) the Compliance Dimension – to combine: iii) the Policy Dimension; iv) the Best Practice Dimension; vi) the Certification Dimension and vii) the Legal Dimension.

2.3.5 Figure 18 below synthesises two ontologies together.

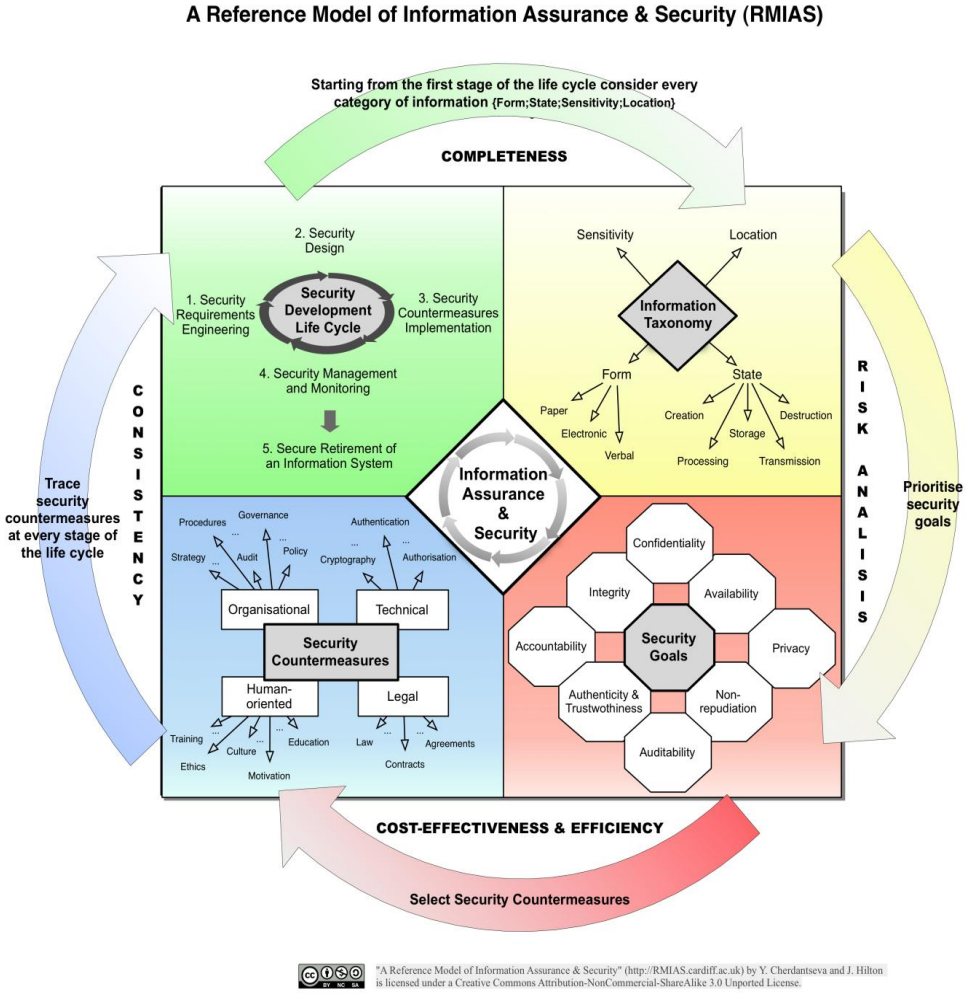


Figure 18: A Reference Model of IA and Security (RMIAS), Source: Cherdantseva and Hilton (2013b)

2.3.6 The researcher recommends a different direction, not seeking to join two disciplines that can be seen to be one (InfoSec) as a subset of the other (IA), but rather showing the roadmap progression leading from

IT Security through InfoSec, through IA to IG (see Figure 24). Security may historically have been an IT issue. However, assurance raises the requirement to a more organisational one, given the importance of valuing information as an asset and the need to protect both reputation and personal privacy.

2.3.7 The researcher contends that the plethora of definitions and terminology has led to confusion for those in a position of having to implement the requirements of IA sufficient to warrant clarification, agreement and streamlining. The confusion can often manifest itself in paralysis in implementing the available guidance or the repeated themes evidenced in many of the government and industry reports that follow after a significant event, breach or incident.

2.3.8 It behoves IA professionals to take stock and ensure that they understand the background and theory before continuing to progress with both professionalisation and with the future *consumerisation* in the context of the IoT, where interconnectivity is the norm, making personal information even more of a commodity (Howard and Prince, 2011).

2.4 Identification of IA Best/Common Practice

2.4.1 Good and best practices have existed for a long time and need to be used (Nanton, 2004). "Best practices" are designed to be vague enough to apply in the general case. They are dictated by consultants, vendors and the security industry as a whole. "Best practices" are activities that are supposed to represent collective wisdom within a field (Shostack and Stewart, 2008, p.36-37). Best

practice is considered to be a business buzzword, used to describe the process of developing and following a *standard* way of doing things that multiple organisations can use. A best practice is a method or technique that has consistently shown results superior to those achieved with other means and is used as a benchmark.

2.4.2 As improvements are discovered a "best" practice can evolve to ameliorate operational outcomes. Unfortunately, however, what is evident is often not even standard practice, but rather a lack of common sense. The Ashley Madison breach highlighted how far education still has to reach, how deeply it needs to be embedded, in order to improve one of the most standard of requirements - password management practices (Whittaker, 2015).

2.4.3 In order to effectively embed IA – in government, in industry and beyond - the goal must be to transform InfoSec into a multidisciplinary field in which technologists work closely with experts in "soft issues" such as public policy, economics, and sociology (Shostack and Stewart, 2008, p.103).

2.4.4 The work of Piatek and Newkirk (2009) addressed many of the questions concerning what is involved in embedding IA into US Department of Defense (DoD) systems being developed, though with the emphasis being on technology enhancements through the system development lifecycle (SDLC), rather than securing business improvements overall. The work of Pappas (2008) reviewed the US DoD approach to IA awareness training in detail, collating a wealth of

resources and articulating the IA challenge in the context of information superiority.

2.4.5 A continual theme throughout the first decade of the 21st century has been that "IA is both art and science"; it needs to be tackled through multidisciplinary efforts (Petersen *et al.*, 2004; Bishop, 2003, p.xxxii-iii).

2.4.6 From a UK perspective, the starting point is a premise of understanding *InfoSec*. On the passing of the thirtieth anniversary of the creation of BS7799, Lacey (2013b) wrote the following:

> Donn Parker of SRI International, and several security audit companies were also experimenting with a set of IT controls which eventually become COBIT prior to the late 1980s when David Lacey joined Shell and by the late 1980s had assembled a collection of around a hundred baseline controls which were published privately for the I4 InfoSec circle which he conceived and founded.

2.4.7 This was an early reference to the longstanding existence of common practice. As referenced by NIST (US NIST, 2001b):

> IA is achieved – and must be maintained – through a process that includes the assessment of threats to an IS, an analysis of the vulnerabilities in the system, an understanding of the impact of a system failure, and the application of technical and non-technical countermeasures to reduce the risk to an acceptable level for the business.

2.4.8 Core to understanding IA is appreciating to what the "information" is referring. The function and responsibility of security personnel is to

protect corporate information assets. Kovacich (1998) addressed the issue of "the value of information", in particular, that it is time dependent.

2.4.9 Barman (2002) pointed out the important concept of *information as an asset*. Peltier (2002) referenced the term "information protection". Two years later, Peltier (2004, p.3) contended that "Information is an asset and is the property of the organization" and also added that an IP "program should be part of any organization's overall asset protection program". This requirement has taken on increasing importance with the ongoing maturation of the InfoSoc. Blyth and Kovacich (2006, p.121) showed this progression over time in Figure 19, showing examples of assets requiring protection, though the researcher contends that the Information rather than the Knowledge age remain the area of greater concern.

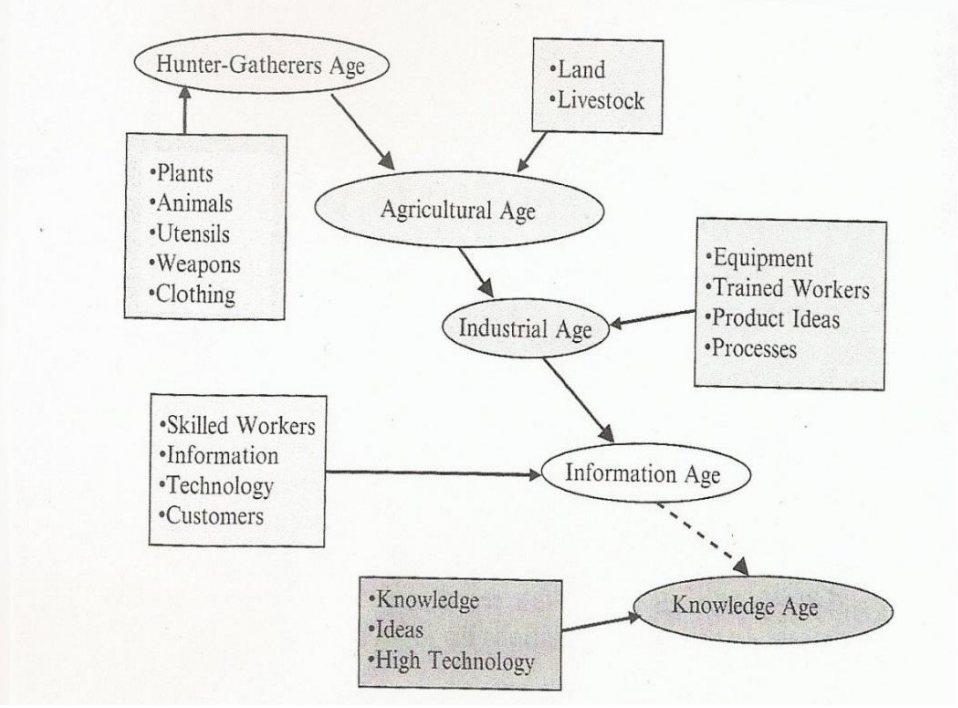


Figure 19: Evolution of the Human Ages, Source: Blyth and Kovacich (2006, p.121)

2.4.10 IA includes those actions that protect and defend information and IS. IA is both a business enabler and a business protector; ensuring users of IS are not unwittingly exposing themselves to unacceptable risk. This has equally been expressed as IA representing a migration from a *preventative* to an *enabling* approach (McFadzean, 2005). McFadzean (2005) contributed to the BoK by producing a brief history of the early part of the 21st century and the progression of IA, particularly with regard to the need to make a business case to senior management for their "buy-in".

2.4.11 The stated benefits of creating a corporate IA culture and corporate IA programme are expected to include (UK Public Administration Select Committee, 2010): i) more assured continuity of business processes and services and of the business itself; ii) greater efficiency and higher levels of performance of internal operations; iii) improved security, integrity, reliability, and utility of IS and data (higher levels of maintenance of the corporate information infrastructure); and iv) more reliable and greater leveraging of the goodwill, trading and support relationships established with partners, stakeholders, customers, investors, government and the public at large.

2.4.12 ISACA brought these concepts together in their Business Model for InfoSec (BMIS), shown in Figure 20 below, seeking to provide an "in-depth explanation to a holistic business model which examines security issues from a systems perspective" (ISACA, 2009; ISACA, 2010a). In the researcher's experience, this is the most holistic and useful, practitioner based operational framework.

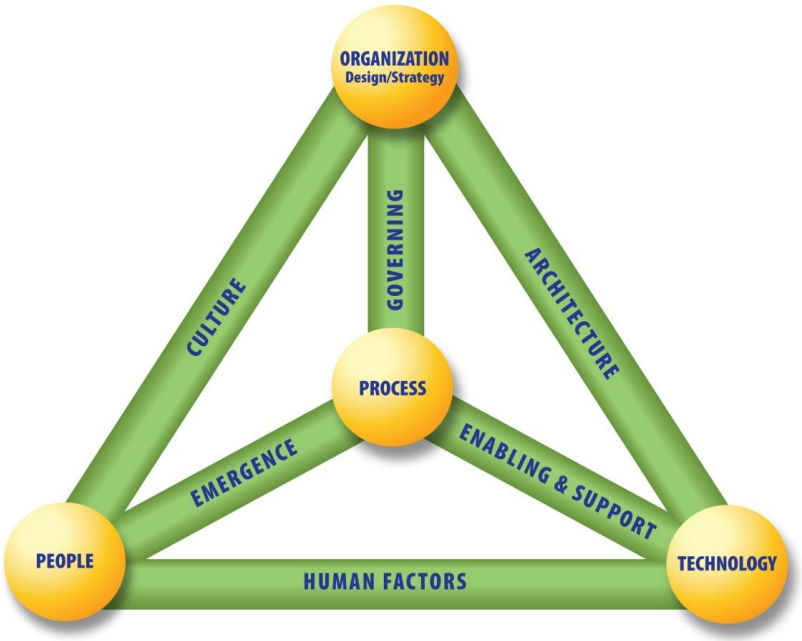


Figure 20: BMIS - the Business Model for InfoSec, Source: ISACA (2009)

2.4.13 There are a number of basic steps found sequentially in most InfoSec standards (ISO 27001, ISACA BMIS *et al.*), which build towards the identification and implementation of an InfoSec management system (ISMS) (Dimitriadis, 2011). These are: i) **Business Impact Analysis** – looking at the impact to the business following the realisation of a threat, usually in terms of the monetary, reputational or legal impact; ii) **Risk Analysis** – the possibility of the occurrence of a security incident is calculated based on a database of security weaknesses. This step needs to take into account technical measures that are already in place to reduce risk and any other complementary controls already available; iii) **Risk Management** – once identified, risks are prioritised in relation to the impact level and business appetite for risk; and iv) **ISMS implementation*** – management framework implementation including consideration of human, cultural, technical, business and

external factors and requires metrics, measurement, and continuous improvements. * The work of Coles-Kemp (2008) provided an extensive review of the understanding and effectiveness of ISMS implementation.

2.4.14 InfoSec requires controls to be selected and implemented, the best of which are *preventive* (in the most obvious sense of preventing any breach of security from taking place in the first instance), such as firewalls, user access control mechanisms, encryption of data and communications, digital signatures, data backup systems and *detective* controls such as intrusion detection systems or security monitoring platforms form the basic components of security architecture. Palmer (2011) provided helpful explanation for the types of controls: i) "Preventive controls ("before the fact") – The most important control type since, if 100 per cent effective (which it never is), none of the others would be necessary – physical barriers, passwords, etc.; ii) Detective controls ("after the fact") - If a preventive mechanism fails, this is the first type of control necessary to identify the facts prior to correction – audit trails, monitoring, etc.; iii) Corrective controls ("before or after the fact") - This type of control is designed to correct a problem once identified – change control, overrides, etc.; iv) Compliance controls ("enforcing the fact") - Compliance controls are designed to keep an organisation inside the law and its Chief Executive Officer out of jail – observing data protection laws, avoiding libel, etc.; and v) Deterrent controls ("instead of the fact") - Designed to advise against certain forms of action - security policy, logon warning,

etc." The various technical controls are usually complemented by a framework of security policies, procedures, and guidelines aimed at controlling the actions of the users to whom they apply (Kesar, 2011).

2.4.15 As an example of further duplication and replication, in 2014, the European Banking Authority (EBA, 2014) proposed new regulations aimed at payment service providers (Hancock, 2015). The security recommendations included: i) segregation of duties in information technology; ii) hardening servers with secure configurations; iii) applying "least privilege" principles to access control; iv) limiting login attempts; v) end-to-end encryption; vi) logging and vii) change management. These elements were already addressed in the PCI DSS (PCI SSC, undated). They were also covered in other financial sector guidance and regulations, as well as in ISO 27001; in the US Federal Information Security Management Act (FISMA); in NIST; in SANS Top 20 Critical Controls; in the UK Governments 10 Steps to Cyber Security; the list goes on.

2.4.16 Ezingeard et al. (2003) described IA as having been "developed by IAAC" which was not untrue. In 2000, the IA Advisory Council (IAAC) was formed in order to further IA research and discussion across the public and private sector and academia. IAAC is a unique partnership between government, industry and academia and its members include some key government policy makers and the research community. Collectively, they developed the subject area and worked with notable bodies such as the Institute of Directors (IoD) to improve organisational adoption.

2.4.17 The Turnbull Report (ICAEW, 1999) and BS7799 (now ISO 270001) were also identified as important influences on the maturation of IA in the UK, although BS7799 was inaccurately described by the authors (op.cit.) as the "Code of Practice for IA Management". It has only ever been an "InfoSec Management" code. In 2007, they updated their earlier InfoSec best practice identification work, represented in Table 1 below, as a comparator of the two particular fields.

	InfoSec	**IA**
Confidentiality	Need-to-know only and protection from unauthorised access	How can ongoing compliance be ensured against regulatory changes or regional variations? What would be the impact on reputation of a breach of confidentiality?
Integrity	Preventing accidental or malicious alteration, corruption or deletion	Can users compare relative levels of reliability if data are conflicting? How does the organisation reduce costs incurred through errors?
Availability	Disaster recovery and business continuity to ensure ongoing operation of existing systems	How can we develop systems that will not be restrictive as the organisation grows, enters new alliances or develops new business?
Identification and authentication	Password access control	Do users keep their passwords secret and regularly changed because they are told to or because they understand the importance of password safety? How can we develop better identification and authentication methods for our stakeholders?
Non-repudiation	Fraud prevention	How can security reduce the organisation's transaction costs? Can transactions be simplified for our customers to increase their value gained from dealing with us, without compromising security?

Table 1: Comparing InfoSec to IA, Adapted from Ezingeard, McFadzean, Birchall (2007), pp.96-118

2.4.18 IAAC (2003m) defined IA as "the certainty that the information within an organisation is reliable, secure and private. IA encompassed both the accuracy of the information and its protection, and included disciplines such as InfoSec Management, Risk Management and Business Continuity Management". This definition focused attention on the centrality of information to holistic business assurance. The endeavour was to alter perceptions such that IA would be seen not as an optional, additional activity but rather as something to be embedded throughout an organisation.

2.4.19 The terminology used was deliberately different from the standard *CIA* triad, using the terms *reliable, secure and private* on the premise that these would mean more at director level (McFadzean, 2005). Further IAAC publications refined the definition:

> IA is a holistic approach towards protecting information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. Although building on the discipline of InfoSec, the concept of IA raises the profile of security as a business critical operational function rather than as a technical support function (Anhal *et al.*, 2002).

The long term goal was to achieve a good level of IA throughout the Digital Society (IAAC, 2002), for the systems and data that people rely upon in their daily lives to be reliable and trustworthy. This meant that IS would protect the data they process, store, and communicate; they would function as they need to; they would function when they need to; and they would function under control.

2.4.20 Another entrant into the IA domain is “Cyber-Physical Systems” (CPS), a 2015 three letter acronym (TLA) from a working group sponsored by NIST in the US, seeking to address the pressing requirements of ensuring assurance across “smart” systems. The term was chosen to denote the interconnectedness between the physical (e.g. kettle, fridge, car) domain and the cyber (the ether) domain and the intended framework is represented in Figure 21 below.

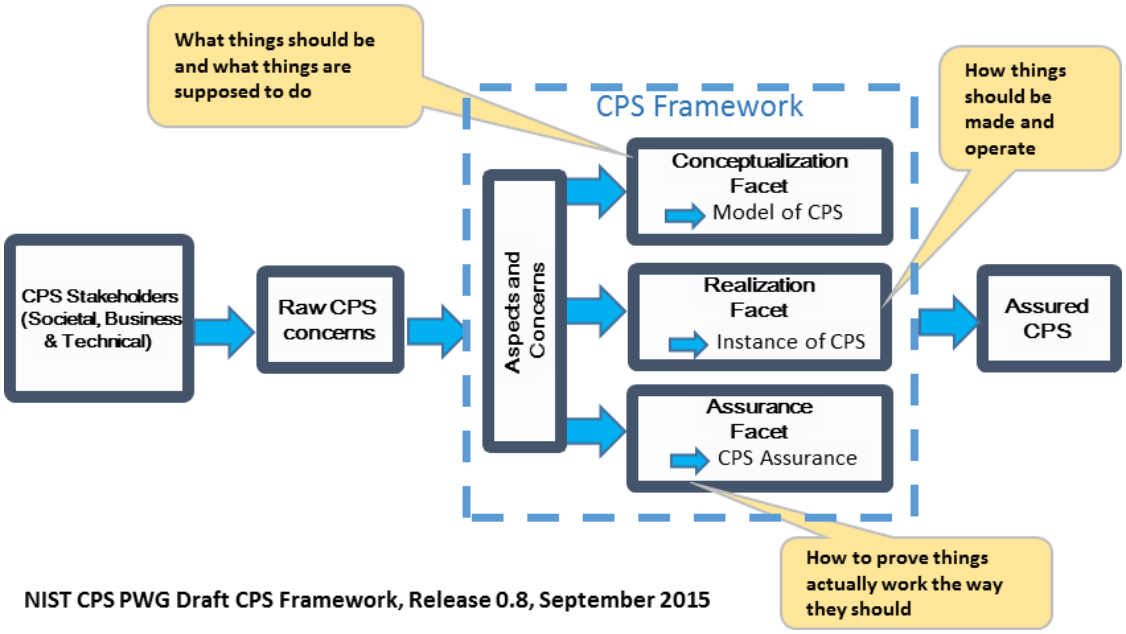


Figure 21: CPS PWG Draft CPS Framework, Source: NIST (2015)

2.4.21 Existing terminology covered these – *Operational Technology (OT)* and *Information Technology (IT)* - and in other areas of the industry, convergence of these two vertical areas of focus had already been taking place. Whilst the work undertaken by the CPS Public Working Group (PWG) provides a worthy framework for operations, and is intended to provide an appropriate reference architecture moving forward, the researcher would contend that without acknowledgement of the existing constructs within which IO are *already* taking place, this

will appear as a *new* activity, will drain precious resources and will therefore dilute existing efforts.

2.4.22 This ongoing entrance of new players and new terminology, new standards and new frameworks, to address existing work done shows a closed system at work, lacking proper interaction continually moving toward greater disorganisation (Koenig, 2012, p.19).

2.4.23 The IA process is cyclical; the risk assessment and risk management plan are continuously revised and improved based on data gleaned from evaluation (reviews) (Walters, 2011). This cyclical work addresses some of the challenges of the complexity and the anticipated unknown unknowns. Reviews provide both causes and effects that can be addressed by the implementation of available standards (safeguards, countermeasures, controls).

2.4.24 The work undertaken by Cornish *et al.* (2011, p.viii) in *Building a Cyber Security Culture* identified clear examples of best practice in action. However, it did not appear to identify the existence of resources such as GetSafeOnline nor CESG as signposts for available resources and for awareness raising efforts. All UK Government departments were encouraged to foster a culture that values, protects and uses information for the public good (UK Cabinet Office, 2010a). Clear principles exist and the UK public sector is well served. CESG and GCHQ only provide advice in many areas, advice that can be and is often ignored. These are the distilled best and common practice required to achieve both InfoSec and then IA, which should be standard practice in all organisations irrespective of sector. This has

been used to assess how well IA activities were being implemented. These Assurance Activities, if adequately implemented, would address the findings of the regular Ponemon Data Breach reports - that the cost of a data breach can be reduced (Prince, 2015) by having i*)* an incident response plan and team; ii) extensive use of encryption; iii) business continuity management (BCM) involvement; iv) Chief Information Security Officer (CISO) leadership; v) employee training; vi) board-level involvement; and vii) insurance protection.

2.4.25 CESG produced ten Assurance Activities - the "10 Steps to Cyber Security" (UK GCHQ, 2015) shown in Table 2.

1	**Secure configuration**	Apply security patches and ensure that the secure configuration of all ICT systems is maintained. Create a system inventory and define a baseline build for all ICT devices.
2	**Removable media controls**	Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing on to a corporate system.
3	**Network security**	Protect your networks against external and internal attack. Manage the network perimeter. Filter out unauthorised access and malicious content. Monitor and test security controls.
4	**User and educational awareness**	Produce user security policies covering acceptable and secure use of the organisation's systems. Establish a staff training programme. Maintain user awareness of the cyber risks
5	**IRM regime**	Establish an effective governance structure and determine your risk appetite – just like you would for any other risk. Maintain the Board's engagement with the cyber risk.
6	**Home working**	Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline build to all devices. Protect data both in transit and at rest.
7	**Managing user privileges**	Establish account management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.
8	**Malware protection**	Produce relevant policy and establish anti-malware defences that are applicable and relevant to all business areas. Scan for malware across the organisation.
9	**Monitoring**	Establish a monitoring strategy and produce supporting policies. Continuously monitor all ICT systems and networks. Analyse logs for unusual activity that could indicate an attack.
10	**Incident management**	Establish an incident response and disaster recovery capability. Produce and test incident management plans. Provide specialist training to the incident management team. Report criminal incidents to law enforcement.

Table 2: Assurance Survey (UK GCHQ, 2015)

2.4.26 However, standards do not establish security, people do. Therefore, similarly, standards will not deliver IA, people will (Ross, 2013, p.4). Good security practice supported by robust systems design remains absent, despite available information, resources, courses and guidance, as well as legislative, regulation and industry changes. However, historical research shows the existence of awareness of many aspects of management, strategy, and leadership.

2.4.27 For example, Aberdeen Group research (2005 cited in ITGI, 2012, p.33) identified that "losses due to ineffective security can be reduced by up to 90 per cent by implementing known, commonly used security practices. This alone should be sufficient to motivate action by responsible management". There are many organisations purchasing equipment and solutions that may not be necessary if more understanding of the available best or common practices, regulation, legislation and available standards existed amongst the involved professionals. "This lack of intellectual honesty has led the entire industry a long way off course" (Howard and Prince, 2011, p.259).

2.4.28 Finally, the impact of organisational politics on the ability to deliver IA is not to be discounted (Pott, 2015 and Valsmith, 2015). This was identified by the work of Peter Drucker (in Stein, 2010, p.60):

> The modern corporation is thus a political institution; its purpose is the creation of legitimate power in the industrial sphere. [...] The political purpose of the corporation is the creation of a legitimate social government on the basis of the original power of the individual property rights of its shareholders.

2.4.29 Information Age infrastructure is founded upon the Open Source Interconnection (OSI) Seven Layer model, shown in Figure 22 below.

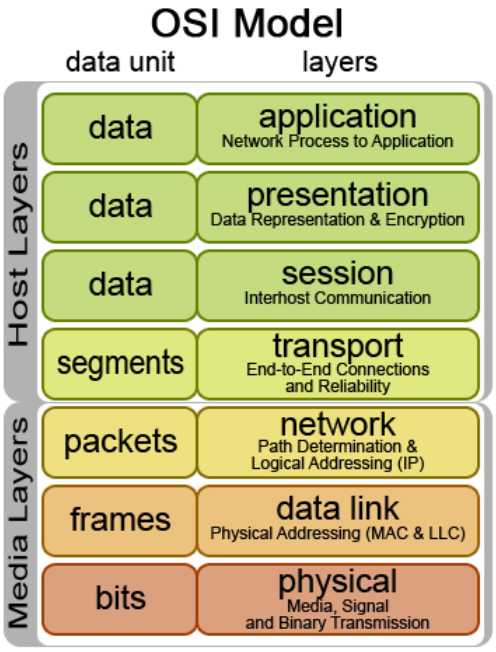


Figure 22: OSI Model, Source: Korah (2006)

2.4.29 However, there are people and psychological layers that need to be considered on top, where politics is occurring between the margins of layers 9 to 11: i) Layer 8 can be considered the business process layer; ii) Layer 9, the human contact layer – also the cognitive layer; iii) Layer 10, the context layer; and iv) Layer 11, the ecosystem layer.

2.5 The Growth and Usage of IA in the UK

2.5.1 Through the review of IA definitions, it has been observed that the UK development has been influenced by its ongoing maturation in the US. IA covers the defensive realm of IO, based on concepts and models that have migrated from the field of IS security (Blyth and Kovacich, 2006).

2.5.2 From 2002, the UK Government's key source of guidance on IA was the UK Central Sponsor for IA (UK CSIA, as was) and it defined IA as: "the confidence that information systems will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users" (UK CSIA, 2002). This is the definition that is consistently used in most central government related publications.

2.5.3 Shanes (2011) identified that assurance is fundamentally about reassurance in the context of operating government systems. Table 3 presents existing UK Government initiatives designed to assist organisations in addressing IA, though without a timeline.

Themes	Activities				
	Web Sites	Guides	Meetings / Workshops	White Papers / Reports	Research and Surveys
Government / Industry Partnership	CESG NISCC DTI	NISCC CSIA	CESG NISCC CSIA	CSIA	NISCC DTI
Governance		CSIA	CSIA		
Regulations and Certification	CESG DTI			DTI	CESG
Professional Standards	CESG		CSIA	CESG	
Business Continuity	CSIA DTI	MOD DTI	CSIA DTI	CESG	CESG DTI
e-Crime	Home Office NHTCU	Home Office DTI	Home Office DTI	Home Office NHTCU	
Warnings, Advisories and Reporting	NISCC CSIA MOD (JSyCC)	NISCC	NISCC MOD (JSyCC)	NISCC	
Security Technologies Best Practice	DTI CSIA	DTI NISCC MOD	DTI CSIA	CESG CSIA	CESG
Security Architecture	CSIA	NISCC	DTI CSIA	CESG CSIA	CESG
Privacy and Data Protection	DCA ICO	DCA ICO		CESG DCA MOD	CESG ICO
Biometrics			DTI	CESG	CESG
Digital Certificates/PKI	CESG		DTI CSIA	CESG	CESG DTI

Table 3: Public Sector IA initiatives, Source: Shanes (2011, p.34)

2.5.4 Corporate Governance was brought to the fore following the Enron scandal where the organisation involved was found to have been remiss in its financial reporting and its auditors were embroiled in the subsequent debacle on the basis of having signed off on accounts that were not a true reflection of the internal reality or risk levels (Turnbull, 2002). Subsequent reporting in the UK included references borne from these events including the Higgs Review (Higgs, 2003), the Smith Guidance (FRC, 2005) and the Financial Services Authority (FSA, 2008).

2.5.5 Vendors such as Microsoft, Oracle and IBM have sought to contribute to increased board awareness of risk management as a result of a breach, an incident, a media report or an event that has brought focus onto the requirements of IA in the context of protecting organisational information and embedding information risk management in order to achieve this. The UK had already been reporting on these issues earlier than the Enron scandal mentioned above – through the Cadbury Report (Cadbury, 1992) and the Turnbull Report (ICAEW, 1999). The latter was successful in bringing the issue of internal control and risk management to the attention of the board; its principles remain the building blocks on which good Corporate Governance is based. Thus it can be evidenced that the need for greater leadership and governance has been a strong theme for a considerable length of time, with regard to information awareness, management, and risk reporting.

2.5.6 Boyce and Jennings (2002, p.170) articulated the stages of the security life cycle thus:

> Often security is thought of as an event rather than a process, as a stitch in time rather than a thread that runs throughout each phase of a system's life cycle. Security is often not considered during the initial planning, design, and development of the system. Attempts to retrofit security into the system after it is developed are typically more expensive and less effective than if it is incorporated from inception. Likewise, security does not end once the system has been accredited and approved to operate under certain conditions. Throughout the system's operational and maintenance phase, the system's compliance with the terms of its accreditation must be verified. Even when the system's life cycle is over, security policies and procedures must govern the secure destruction and disposal of the system.

2.5.7 CESG (2012b), the National Technical Authority for IA, used the US DoD "Five Pillars" to communicate IA as being "essential for safe electronic transactions": i) *Confidentiality* – keeping information private; ii) *Integrity* – ensuring information has not been tampered with; iii) *Availability* – ensuring information is available when required; iv) *Authentication* – confirming the identity of the individual who undertook the transaction; and v) *Non-repudiation* – the individual who undertook the transaction cannot subsequently deny it.

2.5.8 The CESG definition constrained IA in terms of "electronic transactions", missing the human factor(s) of physical security as has been witnessed with the many and varied data losses and security breaches, the majority of which have been as a result of an error on the part of a well-meaning member of staff, not necessarily directly as a result of "electronic transactions". CESG's core role was the delivery of a UK technical capability for IA - addressing IA issues at a software and technology level - and to ensure the supply of appropriate technical solutions, which may explain their more narrow focus.

2.5.9 By 2007, the UK National IA Strategy (NIAS) (op.cit.) (first issued in 2003 (UK CSIA, 2003)), aligned with the Hermann scope of IA definition (paragraph 2.2.36). By 2011, the NIAS aimed, to create "A UK environment where citizens, businesses and government use and enjoy the full benefits of information systems with confidence". The Strategy had several intended outcomes: Government would be better able to deliver public services through the appropriate use of ICT; the UK's national security would be strengthened by protecting information and IS at risk of compromise; and the UK's economic and social well-being would be enhanced as government, businesses and citizens realise the full benefits of ICT.

2.5.10 The aim of the NIAS was to embed IA as a part of everyday business processes, ensuring that there was clear and effective IRM by organisations, and agreement upon and compliance with approved and appropriate IA standards. The objectives of the Strategy were the development and availability of appropriate IA capabilities through the

development and availability of the right products and services; coordinated and appropriate efforts on innovation and research; improved professionalism across all areas of the IA sector and improved awareness and outreach across the UK. However, reaching back twenty years, more than sixty per cent of new computer projects at the time failed in the US and the UK alone, with £58 billion lost through technology related 'teething troubles' (Collins, 1997). Returning to the present day, the breach reporting in 2017, showed that only 37 per cent of UK businesses were taking data protection seriously in the context of the implementation of security best practice (Forbes, 2017).

2.5.11 IA in the UK public sector came of age in 2008 as a result of the government response following the HMRC loss of 25 million records (IPCC, 2008). This event proved to be embarrassing to the UK Government and damaging to the trust of the public in the capability of the government to protect their personal data and provide appropriate assurance as to its ongoing safety and security. In order to improve public perception, 11 reports were issued in 2008 alone, which all highlighted the need for, and the importance of, IA [see **Appendix I, Section 10.21**]. Following on from the reporting, which had identified lack of leadership as a cause for bad IA implementation, the requirement was to embark upon an appreciable cross-governmental culture change, addressing data handling procedures, accountability, and InfoSec awareness.

2.5.12 The prevailing rhetoric had been that Government preferred self-regulation whilst wishing to endorse strong ecommerce as vital for the UK in terms of position and development. However, in response to the breach, Her Majesty's Government (HMG) embarked on a programme of implementing cross governmental mandatory minimum measures for data handling which were to be in place by certain dates and thus target setting and measurements became a part of the lexicon and portfolio of IA operations (Cabinet Office, 2008d).

2.5.13 This led to the development of the IA Maturity Model (IAMM) as a mechanism for measuring the implementation of best practice requirements across six categories (UK Cabinet Office, 2009d; UK CESG, 2010a): i) Leadership and Governance; ii) Training, Education, and Awareness; iii) IRM; iv) Through-life IA Measures; v) Assured Information Sharing; and vi) Compliance.

2.5.14 The researcher created and delivered the internal InfoSec and risk awareness training module delivered across the whole of HMRC in response to the second requirement above and published a book as a result of the experiences. This was referenced in Case Study 2.1 in the Cabinet Office report Protecting Information (Simmons, 2009; Cabinet Office, 2010a).

2.5.15 Using the IAMM was intended to enable the required organisational culture change towards viewing information as an important asset requiring protection. The IAMM is linked with the need to "establish a culture of continuous improvement in IA practice" (Schou and Shoemaker, 2007, p.410). Given the wealth of available, historical

material, entering new "government speak" phrases such as "Through-life IA Measures" clouded the already full vocabulary. This is an example of the UK public sector introducing terminology that is inconsistent with the BoK available to the industry professionals likely to be involved in assisting with the implementation of the required controls, safeguards, improvements etc. As Shostack and Stewart (2008, p.xi) stated: "The classics are classic for a reason – they work!".

2.5.16 Adoption of the IAMM is believed to be essential for successful implementation of IA; it is also mandatory for central government departments. The lack of mandate beyond central government, to local government and other public sector organisations, means that IA is not as embedded as it could be. It is often harder to secure senior buy-in, as there are other priorities that have to be met.

2.5.17 The **IA Chronology, Appendix III** signposts an extensive repository of good practice and available resources of advice, all published long in advance of the 2008 data breach. It was this tipping point that led to the researcher being asked to produce a publication to address the identified challenges (Simmons, 2009), which began the analysis as to why it was that such a volume of available material can be at the disposal of those who require it but that it can appear to be continually ignored in the pursuit of progress.

2.5.18 This behaviour has been at the expense of embedding best practice that would have ultimately helped to reduce the risk of such losses and breaches being experienced, not only in the UK public sector but subsequently in the global private sector too. "Best practices are

simply activities that are supposed to represent collective wisdom within a field" (Shostack and Stewart, 2008, p.36).

2.5.19 The difficulty is often that understanding of how badly a security measure can fail is only realised after a failure occurs: "Success is often silent, invisible or boring. It doesn't make for a good story" (Ibid. p.44). The preparations required for the Year 2000 (Y2K) were experienced by many, yet the end result for some was one of no impact whatsoever, so the effort appeared to be wasted (Nolan and McFarlan, 2005, p.1). However, there is no way to evidence this. There was an extra second (a leap second) in 2015. Again, a number of systems had to be prepared for this event, but there was no material impact. Software is always being improved and citizens, customers, and clients can become inured to the need for and value of constant updates.

2.5.20 Heller (2015) identified the difficulties of always doing the right thing and saying the right thing, but there is a groundswell of concern as to where the lines need to be drawn and where the responsibilities lie. There is a need for people who will challenge the status quo, though to do so can increase risk for both the individual and for the organisation they are employed by.

2.5.21 Information is continually confirmed as being fundamental to the business of government. Effective IA is acknowledged as being core to ensuring the appropriate safeguarding of information assets. Yet there have been many public sector IT projects that have been the subject of delays and excessive costs.

2.5.22 The issue of IT project failures has been being widely researched, reported and written about for decades. Both the Commons Public Administration Select Committee (UK Public Administration Select Committee, 2010) and the NAO (op.cit.) have reviewed government progress into the effective implementation of systems and the security applied to them. The lack of real improvement on the basis of lessons that should be learnt from the available materials continues to be of concern (Collins and Bicknell, 1997; Glass, 1998; Virgo 2011).

2.5.23 On the subject of mandatory measures, the National Health Service (NHS) was ahead of central government in terms of implementing IG in 2002/03, with the NHS IG Toolkit which had already been in operation for a number of years prior to the roll out across central government and beyond as a result of the Data Handling reviews of 2008 (UK NHS, 2015). The NHS was clear that IG was necessary to support the provision of high-quality care by promoting the effective and appropriate use of information (YAS, 2011). Therefore, good practice already existed in parts of the UK public sector – parts that had embraced the breadth of the task and matured to *IG* beyond IA.

2.5.24 In 2009, the UK Government was defining IA as:

> the practice of managing information-related risks. IA is the confidence that information and communication systems will, through their life cycle, protect the information they handle (i.e. ensure the information's *Confidentiality* and *Integrity*), and will function as and when they need to (i.e. information is *Available* as required), under the control of legitimate users. This confidence is

vital, as UK government and business all depend on such information systems (Translink, 2009).

2.5.25 Thus it protects information and IS by ensuring CIA, authentication, and non-repudiation. IA is a business function providing confidence in Pragmatic, Appropriate and Cost Effective (PACE) Risk Management of the Confidentiality, Integrity and Availability (CIA) of Information and IS (UK CESG, 2009f). The NIAS was linked to the Government ICT Strategy with three principles underpinning and enabling the delivery of the IA element of the Strategy: i) **Partnership**: It was acknowledged that public sector organisations would need to work together to deliver the right IA outcomes. In particular, Cabinet Office was to work closely with its key partner CESG and the Centre for the Protection of National Infrastructure (CPNI), to drive implementation as well as to engage with the IA Industry in order to ensure vital success of the strategy; ii) **Professionalism**: There was to be recognised and widespread professionalism in IA encompassing those in risk ownership roles in the public sector, industry partners, and government IA specialists; and iii) **Pace and agility**: were anticipated to become the dominant characteristics of design-to-market delivery of IA capability, evaluation of products and services, response to incidents and management of risk impact (UK Cabinet Office, 2009e).

2.5.26 In 2009, two years after the UK Government formation of a single National IA Framework (op.cit.), the first UK Cyber Security Strategy was produced (op.cit.). This followed after the multiple Data Handling Review (DHR) related reports after the HMRC breach (Child Benefit

data loss in 2007). By 2011, the UK Cyber Security Strategy was launched and supported by a £650 million central government investment programme.

2.5.27 Parker and others have been, for over forty-five years, trying to aid understanding of risk, probability and the incentives required to encourage people to do the right thing (more recently referred to as "human factors"). Therefore, it is disconcerting that industry and business continue to experience breaches and incidents. A correlation has been analysed between breach activity and revenue growth (Jaffray, 2016). The security industry profits from insecurity in computing devices sufficient to lack incentives to fix what is known to be broken. This means that principles of professionalism are forgotten. Ongoing data breach and loss volumes can be traced back to bad system design (Hulme, 2012, referencing the work of Koppel). So the more software problems there are, the more continual employment there will be for software engineers.

2.5.28 The implication is that there is deficiency in the approach, the implementation or the understanding (Lacey, 2013b). It is clear that "somebody must pay for broken security and somebody must reward good security (only then will things start to improve). Determining who is who, which is which, and how best to apply these concepts is a matter for government." (McGraw and Arce, 2010) However, Room (2009, p.186) posed the thorny question "does the publication of official reports actually make any difference on the ground?".

2.5.29 These core elements are supported by human needs, as represented by Maslow's Hierarchy in Figure 23 below:

Need	Offline (Maslow)	Online Communities
Physiological	Food, clothing, shelter, health	System access; the ability to own and maintain one's identity while participating in a web community
Security & Safety	Protection from crimes and war; the sense of living in a fair and just society.	Protection from hacking and personal attacks; the sense of having a "level playing field"; ability to maintain varying levels of privacy
Social	The ability to give and receive love; the feeling of belonging to a group.	Belonging to the community as a whole, and to subgroups within the community.
Self-Esteem	Self-respect; the ability to earn the respect of others and contribute to society.	The ability to contribute to the community, and be recognized for those contributions.
Self-Actualization	The ability to develop skills and fulfill one's potential.	The ability to take on a community role that develop skills and opens up new opportunities.

Advancement in Hierarchy

Figure 23: Maslow's Hierarchy of Needs applied to the online world, Source: Kim (2000)

2.5.30 Unless these human aspects are acknowledged and addressed, achieving Objective 4 of the UK Cyber Security Strategy is unlikely. As a result of the dominant narrative, there is a contingent impact on the culture of an organisation in terms of its willingness to adopt the messages provided and embed the best practice advice, which will be explored in further detail in future work.

2.5.31 The researcher contends that the change in dominant narrative from IA to cyber has had a dilution effect on adoption and understanding of existing dogma. Cyber space is often referred to as the area of focus for policy development in the 21st century and yet for the criminals, their focus is not limited to the Internet. It can involve many technological systems that may or may not be connected to the World Wide Web. Criminals are more than content to use "threat vectors"

that exist outside of government agencies' jurisdictions due to near-sighted policies that have not kept pace with those technological developments.

2.6 Conclusions

2.6.1 It can be seen from this review that practitioner literature has made an important contribution to IA understanding. InfoSec was not the focus of searches as this would have rendered the scale of the task all but insurmountable. Corresponding resources are available, particularly in the work of Cherdantseva and Hilton (2014). Whilst considerable continuity of approach has been evidenced, differences in pronouncements by advisors, regulators and other bodies have also been identified. The Literature Review has shown incremental definition maturation over time. Definitions are temporally dependent, given that each concept is subject to a process of evolution on the basis of educational progression and experiential learning.

2.6.2 IA definitions have been compiled in **Appendix I: Table 29**; however, the following definition formed the corner stone of the research:

> Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities (US DoD 3600-1, 1996 cited in Herrmann, 2002).

2.6.3 The language of IA starts with the language of InfoSec. The majority of the literature reviewed described the development and implementation of InfoSec; even that which was entitled **IA**, in the main, referenced **InfoSec** at its core. There was a school of thought that the terms remain interchangeable and that the distinction is between the sectors, even at some points reflecting that, in the UK, IA is to the public sector as InfoSec is to the private sector (Blyth and Kovacich, 2006; Lacey, 2010; Virgo, 2011).

2.6.4 Blyth and Kovacich (2006) were in accord with the UK CSIA definition but stated that they are content for the reader to make their own mind up once they have completed reading the work. The work of Ilies and Boaru (2011) contains an interesting view of the terminology interplay between InfoSec and IA, from an IS standpoint, in the context of NATO. The statement that IA "determines all information flows" is challenging, though the identification of the significance of information classification is important. In the experience of the researcher, this is unhelpful from the perspective of a practitioner.

2.6.5 Any lack of clarity creates risk as it devalues the existing definitions. Identified IA theory discusses the five pillars upon which a successful IA programme is grounded: availability, integrity, identification, confidentiality, and non-repudiation of information assets. Fundamentally, IA is understood to be the *confidence* that information assets within an organisation are maintained reliable, accurate, secure and available when required. This was a reference object constellation from InfoSec enhanced to IA through the five pillars. The

adoption of cyber securitization has had no equivalent explanation of any distinction as to the description of relevant cyber security best practices.

2.6.6 Palermo (2011) referenced the difficulties raised through the use of "loose terminology". A Wikipedia search for cybersecurity during the timeline of this research continually pointed to "computer security", implying interchangeability. Practice literature reflects that different assumptions and situations evoke different responses based on the provided definitions. This has led to both dilution of understanding and impedance of successful implementation. Future locus of attention needs to be on the integration of multiple complex systems in order to reduce confusion. Awareness of this challenge will assist both academia and practitioners to reach a better understanding as well as developing more appropriate analytical language.

2.6.7 Similarly, in the opinion of the researcher, formulation of new models, deliberately joining InfoSec and IA together, does not adequately address the identified gaps in understanding; rather it perpetuates the prevailing confusion by adding more "communication noise". The researcher would contend that this does a disservice to the depth that can be found in the available IA history and practice, as documented herein, and the benefits that can be gained from understanding this and thus implementing it properly and comprehensively.

2.6.8 The Literature Review initially intended to focus on the area of IA in the UK Public Sector, providing a thorough review of 2000 to 2010, years which were the most volatile in terms of information growth and

expansion and thus simultaneously increased information risk. However, what was most illuminating was the identification of so many relevant and important resources spanning previous decades, addressing the information sciences and beyond. These added to the BoK and depth of understanding of the IA domain, creating an extensive and wide ranging Bibliography. Part of the work included a review of the outputs from IAAC from their inception in 2000 through to the present day (2017). The impact of their output has been vital to the understanding and maturation of IA in the UK. The researcher has interwoven this review into the ***IA Chronology, Appendix III***.

2.6.9 As Collins and Bicknell (1997, Author's Note) pointed out, "it is possible to avoid disasters by reading a book". There is plenty of valuable resource material available. However, it appears that practitioners in vital roles and professional positions are lacking in the skills to identify and benefit from them.

2.6.10 There is much that has been written about IM *outside* of the security arena and it is being missed by those involved in maintaining the BoK for InfoSec and IA. This can be evidenced in the various BoK repositories available. The contents do not include nor allude to IM as being a core subject area of value in the context of InfoSec. As neither InfoSec nor IA is considered to be fully fledged scientific disciplines in their own right, there is a paucity of academic resources upon which to draw.

2.6.11 In order to position IA effectively, there needs to be appreciation of other related disciplines. In the 1970s, the US Government

commissioned a report into information usage – both paper and electronic - which popularised the concept of IM (Kahn and Blair, 2009). Kahn and Blair (Ibid. p.14) provide a history of the IM realm as far back as 1943 and reference a definition of InfoSec which shows how narrowly it was viewed, understood, nay required at the time: "ensuring that the valuable information is accessible only to those authorised to see it; and ensuring its trustworthiness". Information has to be safely stored in order to be of use for future generations.

2.6.12 IA is part of the cross-disciplinary domain that is IM. In the publication by Best (1996, p.136) there was acknowledgement that "Probably the greatest technological problem affecting IM is that there is so much technology about and it keeps changing very rapidly". The same could be said of InfoSec and IA. This is not something that is widely understood by those responsible for delivery of InfoSec solutions. It is important for any organisation to know its processes and its information needs. Best (1996, p.137) articulated that "IM is NOT just another name for information technology". Without knowing this context, it is difficult to overlay security and assurance needs.

2.6.13 The Literature Review led to the identification of themes that were the focus of the research questions, detailed historical contextual and discourse analysis following surveys, interviews, and case study research. In order to constrain the scope of the research, the themes were prioritised (high, medium and low priority) and subsequent sections of *Chapter 4* reflect the findings in these areas: i) Terminology (understanding of IA); ii) Drivers and Obligations (to

implement or achieve IA); iii) Standards and Measurements (covering best practice); iv) Impact of Culture and Politics (addressing organisational change) – on the management of information risk – both internal to an organisation as well as external (Low priority at the outset, but grew higher through the Grounded Theory process) – addressed by the work undertaken by Shanes (2011) in reviewing IA in the MOD. This area included elements of Management theory (to help understand the first two) (Medium priority); v) Professionalism of ICT and IA (High priority) – note: the focus is on IA, not on ICT; vi) InfoSoc (reflecting the present context and the impact of the IoT; and vii) Barriers (to achieve successful IA implementation).

2.6.14 For ongoing reference, the researcher has viewed the continuum from IT Security, through InfoSec, through IA to IG, represented in Figure 24 below:

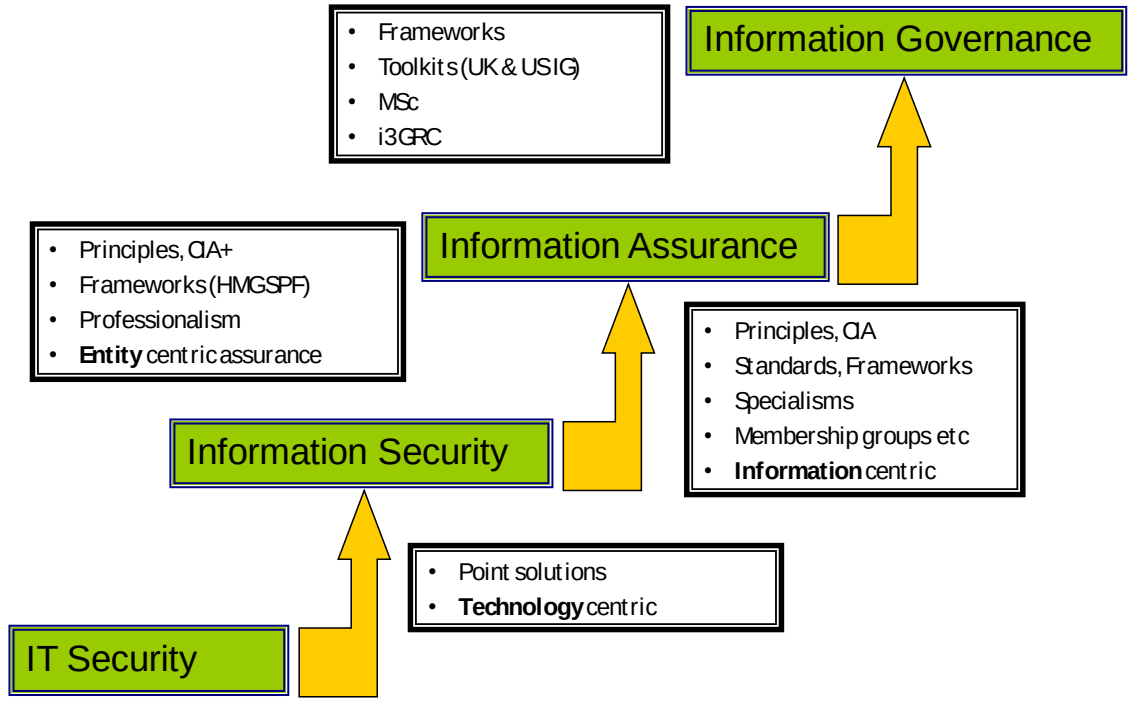


Figure 24: IP Continuum

3 RESEARCH STRATEGY

3.1 Introduction

3.1.1 In this chapter, the reasons for the research strategy, the chosen methodology and the identification of the research questions are addressed.

3.1.2 The underlying theories that supported this research are: Critical Theory, Design Science Research Theory and Chaos Theory, but the most important and predominant was Systems Theory – through the lens of management, organisation and integration.

3.2 Research Questions

3.2.1 The research questions are listed in Table 4 below alongside the methods utilised to answer these:

Q#	Question	Methods Utilised
1	*Can IA professional practice be improved through enhanced IA understanding?*	Historical Research Survey and Interviews Contextual and Discourse Analysis
2	*How has the extensive body of knowledge influenced professionals?*	Survey and Interviews Contextual and Discourse Analysis
3	*Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec through to IA?*	Contextual and Discourse Analysis PAR/Case Study
4	*Is it possible to produce a framework suitable to support the route from IA to IG?*	Grounded Theory PAR/Case Study

Table 4: Research Questions

3.3.2 Further questions arose from the literature review and the ongoing iterative content and discourse analysis, as follows: i) What are the origins and original definitions of IA?; ii) Are these definitions understood at appropriate organisational levels in order to effectively implement IA requirements, both now and as they develop over time? iii) How does the ability to apply learned intelligence, or not, support the advancement of the InfoSoc?; iv) What impact has change of political leadership in government had on the direction of IA across the UK public sector – in the context of policy making and professional practice? v) What other barriers (constraints) to successful implementation of IA can be identified through historical review and research of available materials, interviews, surveys and observation of human interactions?; vi) How do the answers from the previous questions support the development of the IA profession?; and vii) What should the ethical requirements be for IA professionals?. These subsequent research questions represented the structure for the development of the survey questionnaire.

3.3 Approach

3.3.1 This was a mixed method research study, utilising a range of qualitative approaches, including: i) Extensive **content/textual analysis** to extract the critical success factors from available secondary sources including journals, books and reports; Desktop Research, Desktop Analysis [Historical Research, Grounded Theory]; ii) **Survey** research was undertaken in order to identify primary source data, using the free association narrative discourse analysis of survey

questionnaires and interview notes with a view to supporting a new grounded theory (Hollway and Jefferson, 2008). and analysis; iii) **Interviews** (unstructured, informal, freeform, conversational and discursive) were undertaken with key practitioners in both private and public sector organisations in order to provide depth to the survey results; iv) **Unstructured observation**, capturing "insider" knowledge through **PAR**, observing and detailing illustrative incidents. Qualitative researchers study people by observing them in their natural settings, or by analysing the cultural symbols they use. This brings together a variety of empirical materials (case study, personal experience, interview, participant observation, historical analysis of available texts) that describe routine and problematic moments and meanings.

3.3.2 There are a number of data collection tools that could have been used to collect primary data, of which the first two were chosen for this research: i) Semi-structured person to person interviews; ii) Telephone/Skype interviews; iii) Postal questionnaire; and iv) Electronic survey.

3.3.3 Two **case studies** are presented for analytical purposes – one public sector [**CS1**] and one private sector [**CS2**]. The PAR was field research, conducted in natural settings in order to collect substantial situation information; utilising inductive reasoning from observations through to formulation of a **grounded theory** to explain the phenomena identified in the field of exploration. [PAR/Case Study]

3.3.4 For the first phase of the research, a Literature Review was undertaken utilising historical research methodology, as a systematic

process designed to collect and "objectively evaluate data related to past occurrences to arrive at conclusions about the causes, effects, or trends of past events that may be helpful in explaining the present" (Nel, 1983, in Scott, 2004). This historical analysis of identified IA BoK drew inspiration from ethno-methodological critique of official statistics and relevant documentary sources. The literature search was focused on both academic and practitioner published research spanning decades, explicitly related to *IA* as opposed to *InfoSec* (see **Appendix I, Section 10.18** for a list of resources utilised, including **Table 9**). The Literature Review was deliberately broad ranging in order to evidence the available volume of material from a number of different sources, across a historical timeline. Historical research was conducted to produce a chronology of IA.

3.3.5 Secondly, the findings of the Literature Review were utilised to define the themes which guided the investigation, leading to the creation of the questions that were posed to respondents during the interviews. This approach was in line with that described by Hammersley and Atkinson (2007, p.3): "The analysis of data involves interpretation of the meanings, functions and consequences of human actions and institutional practices, and how these are implicated in local, and perhaps also wider, contexts.", providing greater depth of understanding and interpretation of the phenomenon under review.

3.3.6 The contextual analysis of existing definitions found in the Literature Review, the results of two related surveys and interviews, alongside PAR in two case studies collectively led to the derivation of a single

graphical representation of a proposed new framework - Integrated and Informed Information Governance, Risk, and Compliance – i3GRC™ using Grounded Theory.

3.3.7 Ongoing literature searches, reviews, and analysis were undertaken in parallel with the ethnographic PAR. As the research gained momentum, and some research questions proved difficult to answer, often a change of direction or an additional type of literature was included in order to try and gain a different perspective on the problem(s).

3.3.8 The research framework applicable is outlined in Figure 25 below. Whilst the steps are numbered in the diagram, the approach need not be consecutive in order to achieve the desired outcome (Johnson and Christensen, 2005).

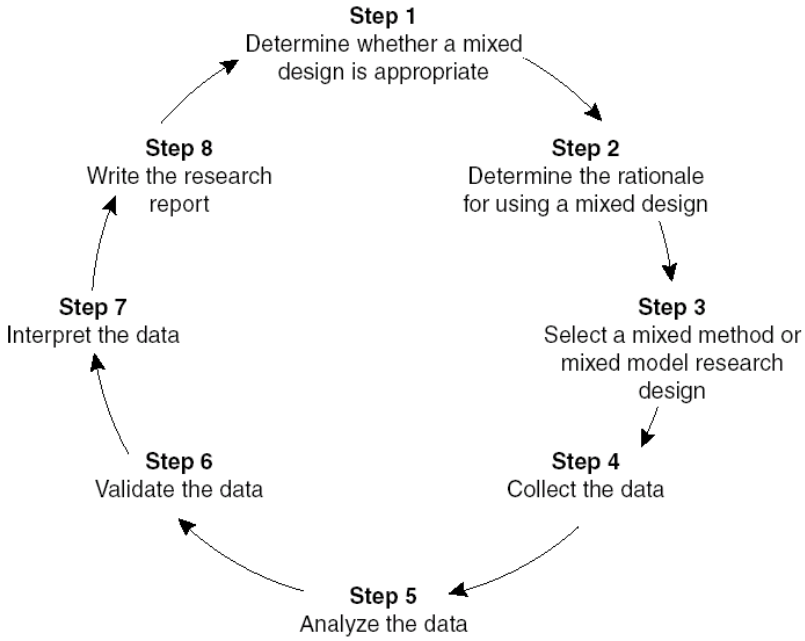


Figure 25: Mixed Research Study Steps, Source: Johnson and Christensen (2005)

3.3.9 The researcher has been part of what is observed; spent considerable time focussed on meanings; sought to understand what was happening; analysed the totality of each situation, and developed ideas through induction from evidence. This has resonance with the Design Science Research Method, represented in Figure 26 below.

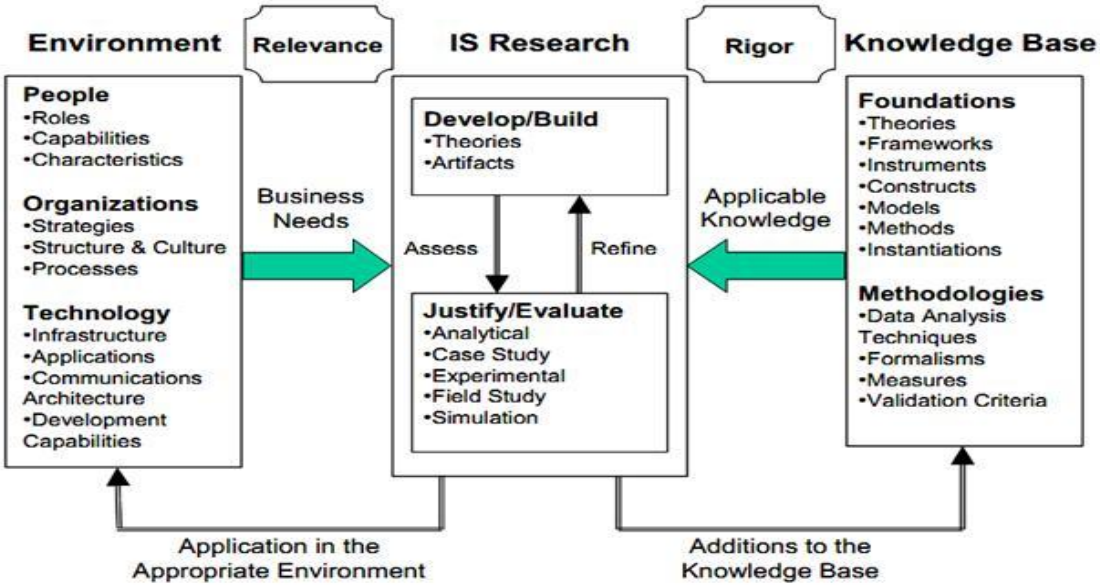


Figure 26: A Design Science Research Methodology for IS, Source: Peffers (2007)

3.3.11 An IA framework starts with a focus on PPT, as represented in the Environment column on the left of the model. The research used the available Knowledge Base (right column) to influence the analysis and stimulation for change within this IS research (middle column).

3.4 Review of Chosen Methods

3.4.1 PAR was chosen for the case study particularly because it is an exploratory and flexible method of research. A case study method is an "appropriate way to research an area in which few previous studies have been carried out", (Benbasat, Goldstein and Mead, 1987, p.370).

3.4.2 Participant observation, ethnography, and fieldwork were used interchangeably (Silverman, 2009) in order to understand the public and private sector cultures and the impact of the various research themes identified. This was a *reflective* process with the ability to impact on wider teams available to the researcher. Reflective practitioners are professionals who systematically improve their understanding of their worlds through reflection on their activities, with the support of their peers (Schon, 1983 in Fisher, 2007).

3.4.3 In **analytic ethnography** the researcher attempts to provide answers to questions about life and organisation, striving to pursue the study in an unfettered or naturalistic manner. The researcher utilised data based on a deep familiarity with the setting that was gained by personal participation and developed a propositional analysis over the course of the research period (Miles and Huberman, 2002, p.137).

3.4.4 PAR methods are applied where the researcher attempts to "obtain practical results of value to groups with whom the researcher has allied him/herself while at the same time adding to the body of theoretical knowledge" (Galliers, 1985, p.282). PAR aims to contribute to practical knowledge of participants as well as scientific knowledge, due to a "joint collaboration within a mutually acceptable ethical framework" (Rapoport, 1970, p.499). In addition, there should be a mutually satisfactory outcome between the researcher's interests of theory and the organisation. The researcher carries out the research as a participant and not as an observer. This method is characteristic of anti-positivism and interpretative or critical research.

3.4.5 According to Susman and Evered (1978), PAR follows a five phase cyclical process: diagnosing, action planning, action taking, evaluating and specifying learning. The researcher's task is to identify the problem area and aim to develop a working hypothesis or predictions that imply a goal and a procedure for achieving it (Baskerville, 1999 and Brewer, 2007). The evaluation phase refers to the assessment of the instructional strategy or technique. The activity "specifying learning" is formally undertaken as an ongoing process to acquire new knowledge. This was encapsulated in a publication by the researcher (Simmons, (2012a) highlighting information loss and data breach incidents and lessons learnt.

3.4.6 The whole process is iterative, like the hermeneutic circle (Brewer, 2007), deconstructing prior conceptions of the phenomenon (of IA), critically analysing how it (IA) has been studied and how it is presented and analysed in the existing research and available literature.

3.4.7 The underlying problem of the PAR method is that "it cannot be wholly planned and directed down a particular path" (Checkland, 1991, p.153). Checkland concludes that the researcher might express his own aims, but is not able to implement them with certainty in the experiment. However, PAR develops the researcher's competency and the testing of findings through critical professional discussion helps to provide holistic and inclusive reflection of the subject (Fisher, 2007).

3.4.8 The researcher agrees with Wadsworth's description of PAR as being "like the discovery phase of any science" in that it "knows it is coming

from somewhere and going to somewhere, even though it does not know in advance where *precisely* (sic) it is going to end up or what the new state will look like" (Wadsworth, 1998).

3.4.9 Lewin expanded on PAR as being appropriate for organisational development, believing that the motivation to change was strongly related to action and thus if people were actively involved in decisions affecting them, they were more likely to adopt new ways of thinking, behaving and acting (Lewin, 1946 in O'Brien, 2001). This is a central tenet for IA practitioners with regard to InfoSec awareness programmes and so the synergy is valuable in this research context. Through the use of PAR, the researcher was able to actively influence outcomes by implementing IA best practice to a mature level in a manner that moved it beyond reflective knowledge creation.

3.4.10 The core reference group for this research has been key members of IAAC. This was been a valuable synergy of interested parties in order to ensure that the researcher remained grounded and provided useful outputs. The **IA Chronology, Appendix III**, was utilised as part of IAAC 10th anniversary collateral.

3.4.11 Memo writing has been conducted in order to follow the lines of inquiry that have resulted from investigation of the subject. Many existing frameworks were reviewed in order to progress through the lines of discovery and interrogate the relationships between concepts (Miles and Huberman, 2002).

3.4.12 In the researcher's opinion, the richness of the patterns identified was best described using a narrative rather than numerical analysis. The

full thesis acts as a primary narrative; a lengthy document telling the story of the phenomenon researched in a comprehensive way. It is from this story that the grounded theory was distilled, through the iterative process reaching a conclusion in January 2015 with the realisation of the need for i3GRC™ as being the next stage on the IP roadmap. One of the core principles of Grounded Theory is that "all is data" (Glaser, 1998). In other words, everything that has been learnt through the research process presents itself as data for further investigation, analysis, and study. As a result, the researcher has been embedded within the IA industry for nearly two decades and has utilised a *constructivist grounded theory* approach.

3.4.13 The process has involved constant review and presentation of the resulting themes seeking paradoxes or contradictions, studying both the absence as well as the presence of IA understanding, engaging in abstract concept discovery and categorisation of the evidence collated throughout the process. Many who, why, what, where and when questions have been asked and, to some extent, answered. However, in dealing with a wicked problem (Rittel and Webber, 1973), it is possible that more questions have been identified than answers found. These are extrapolated in the **Research Findings** (**Chapter 4**).

3.4.14 Historical criticism is a branch of literary analysis of the nineteenth century that seeks to investigate the origins of a text. The historical method of research applies to fields of study encompassing origins, growth, theories, crisis etc.: "History is our collective memory. The ability to utilize history and extract useful generalizations and theories

is uniquely human. Without a record of the past we are left to navigate life's course without the aid of those who have gone before us" (Education Research, 2010).

3.4.15 This methodological approach was utilised to show the links between reports, publications and texts found during the Literature Review and to analyse their impact on IA development. By seeking historical understanding of IA, it should be possible to offer a valuable perspective with which to view present circumstances, perceptions, and uses of IA. History helps understanding of the sources of contemporary problems, how they arose and how their characteristics unfolded through time. It also identifies the solutions that worked in the past and those that did not (Mason, McKenney and Copeland, 1997a). Historical research offers perspectives on phenomena that are unavailable by any other methodological means. The results reflect the cultural circumstances and ideological assumptions that underlie phenomena and the role played by key decision makers together with long-term economic, social and political forces in creating them (Ibid. 1997a).

3.4.16 Of the key schemas of historical thinking (cyclical, providential and progressive) (Gilderhus, 2006), the cyclical school was the most appropriate for this study as it accepted that history repeats itself on the basis that essential forces of human nature are unchangeable and humans make mistakes over and over when confronted with similar or identical situations. Placing the researcher and the subject at the centre of the research process, the phenomenon is captured,

bracketed (to interpret meaning), constructed and contextualised. The intention was to bring the topic into a sharper focus as interpretation laid the groundwork for a deeper understanding (Miles and Huberman, 2002, p.353-360). Stanford (1986) articulated the historical cyclical approach used by the researcher, Figure 27 below.

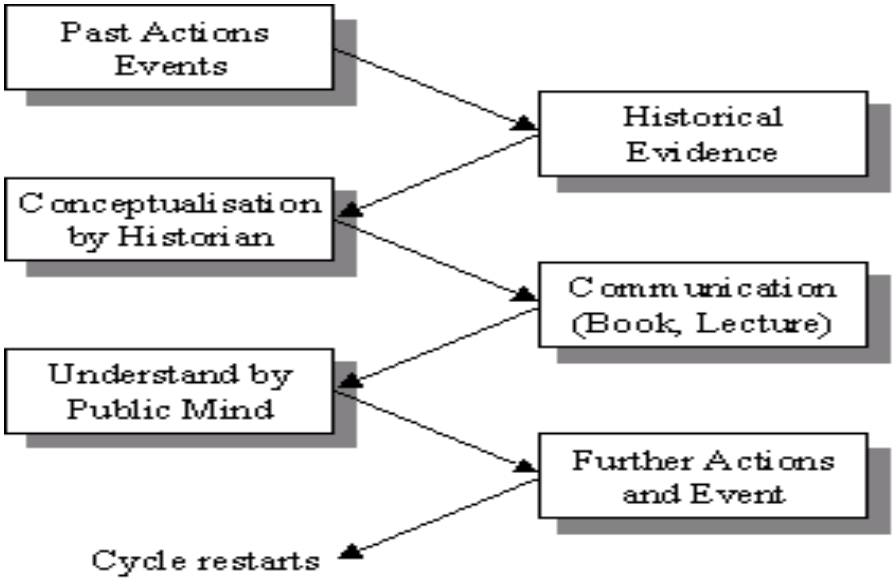


Figure 27: Structure of History, Source: Stanford (1986)

3.4.17 There are a number of steps to be followed which have consistently been referred to in literature: i) the *recognition* of a historical problem or the identification of a need for certain historical knowledge; ii) the *gathering* of as much relevant information about the problem or topic as possible; iii) if appropriate, the *analysis* of evidence and forming of hypothesis that tentatively explains relationships between historical factors and the drawing of conclusions (*synthesis*); and iv) the *recording* of conclusions in a meaningful narrative (*exposition*) (Busha and Harter, 1980).

3.4.18 The main stance this historical research has taken is didactic, seeking to be instructive, teaching a lesson. There has also been a Socratic element, establishing the "why" of historical events that have impacted the development and maturation of IA to date through shared learning and clarification of the known unknowns. The testimony of peers and industry experts from IAAC has been cross checked in order to filter for accuracy. This involves heuristics - the rigorous collection and organisation of the most pertinent collected evidence, the verification of the authenticity and veracity of information and its sources in order to generate learning.

3.4.19 Finding primary sources was relatively swift given the low volume of IA *specific* material available. However, finding the secondary sources was more challenging, particularly as a result of the change in UK Government in May 2009. A number of previously available web links for key useful and valuable resources on IA were removed rather than sent to The National Archives (TNA) repository.

3.4.20 The scope is not as broad as many other historical reviews might necessarily be. Experience and testimony are the grounds for historical certainty. The researcher's experience has already been identified as being fundamental and core to this process, with issues of subjectivity and reflexivity being recognised as influential to the research. Historical research also uses inductive reasoning approaches to build theories that draw conclusions about events, interpreting and observing phenomena – thus the formulation of the

new model, i3GRC™, designed to embody all of the research analysis and findings.

3.5 Research Assumptions

3.5.1 The research questions were constructed upon a number of parallel assumptions: i) *ontology* (the nature of information, available shared understanding of common vocabulary); ii) *epistemology* (human knowledge and how it can be achieved); iii) *research methodology* (the preferred research methods); and *ethics* (the implied values of the research).

3.5.2 The highest level assumptions were as follows: i) subjectivity is inherent, with the attendant threat of researcher bias: the researcher found evidence from the past that supports views expressed today; multiple sources of evidence and corroboration were continually sought in order to reduce this bias; ii) participant observer has affected the phenomenon being studied: changes have occurred; and iii) participant observer has lived in the setting and defers to the culture: this occurred in both Case Study examples.

3.5.3 Under the *epistemological assumption*, the researcher interacted with the object of research and there can be a resultant effect on that object. Findings were created through interaction between the researcher and the researched.

3.5.4 Under the *axiological assumption*, values have a role to play in influencing the outcomes. The researcher was not reluctant to be

openly passionate about pursuing the project and this aspect is dealt with in the Reflexivity section.

3.5.5 The *methodological assumption* requires close interaction between the researcher and respondents. This was the case during the research phase itself, particularly the case studies. Methods included long term observations, free association narrative and conversational interviews and content analysis of documents – analysing the speech acts used rather than the structure of the content.

3.5.6 For a *rhetorical assumption*, the researcher was sufficiently embedded and involved within the object of research that the results were reflected back at regular points throughout, seeking peer review and agreement prior to proceeding.

3.5.7 This research assumes that both the reader and the survey subject already have some appreciation for the background of both IT Security and InfoSec. The work carried out by Cherdantseva and Hilton (2014) squarely addressed the InfoSec definitions space. The researcher further assumed that it is understood and appreciated, or at least would be by the reader who completes the Literature Review, that IA is an important step along a roadmap towards IG and needs to be understood in this context, and within the wider scope of the InfoSoc.

3.6 Research Paradigm

3.6.1 The researcher used an iterative socially constructivist, inductive, design science research approach, in a critical realist ontology, with an interpretive epistemological paradigm. Interpretivism acknowledges that the world is complex and dynamic and is being interpreted and

experienced by people in many differing ways and is impacted upon (both positively and negatively, as shown within the research body itself) by their social context and the wider social systems within which they are operating. Knowledge was constructed based not only on observable phenomena but also on subjective beliefs and understanding of the background to IA and its industry usage and placement.

3.6.2 Historical research requires interpretation of the information and the interpretivism aspect was linked with elements of linguistic study and cultural anthropology in the context of IA and its understanding, usage, and implementation in the UK public sector.

3.7 Reflexivity

3.7.1 Reflexivity means that the researcher remains in an asking or questioning stance throughout (Miles and Huberman, 1994) but also that an individual researcher can have difficulties, being "beset with self-delusions" (Miles and Huberman, 2002, p.119). Analysis of data collected contained a subjective element and was not value-free (Abercrombie, Hill and Turner, 2000, p.372). Miles and Huberman (2002) stressed that subjectivity is a "natural and necessary element of evaluation, which calls for no apology" (Ibid. p.125).

3.7.2 Due to the ethnographic nature of this research, it is important to acknowledge that the researcher's own beliefs and objectives have influenced how the outputs are shaped (Gilbert, 2008: 512 [in Young, 2008]). The researcher cannot be disentangled from the research process, having been embedded within the InfoSec and IA industry for

almost two decades. However, any assertions made have been guided by empirical survey evidence and PAR experience.

3.7.3 The researcher strove to ensure that these risks were minimised by seeking peer review when appropriate, e.g. through the publication of books, papers, presentations etc. The theory constructed is sensitive to the political, economic and geographical context within which the world is operating, particularly the UK.

3.7.4 Reflexivity was borne in mind with regard to political opinion with changes of government. From the outset, the political landscape was recognised as being of importance to the understanding of the terminology used and the implementation of government policy, both elements being fundamental to the research outcomes.

3.8 Other Methodology Considerations

3.8.1 **Systems theory** had a significant sphere of influence as a result of the interdependence and inter-relationship of many of the concepts that form part of this study (Boulding, 1956) particularly the integrated system theory as presented by Hong et al (2003).

3.8.2 The approximate return of a system to its initial conditions – **recurrence** - was identified as an important element throughout the Literature Review, particularly as most of the publications reviewed returned to the core of the original InfoSec management standard (BS7799, now ISO 27001) as the frame of reference for discourse. Recurrence is an understood element of **Chaos Theory**. This field of study is increasingly being used to analyse organisational development, as it relies on the concept of uncertainty as being central

to the influence of change (Spender, 1996). Positively, this "enables a researcher to grasp meaning and respond intellectually (and emotionally) to what is being said in the data in order to be able to arrive at concepts that are grounded in data" (Corbin and Strauss, 2008, p41). The chaos paradigm has replaced the Newtonian reductionist paradigm and the researcher's experience mirrors this. Review of complex systems requires new thinking in order to deal with the limitations reached (Dekker, 2011, p.188).

3.8.3 Also of relevance was the theory of **Complex Adaptive Systems (CAS)** (Holland, 2006). CAS are systems that are networks of interactions and relationships. They are flexible and fluid, adaptive and changing as a result of individual and collective behaviour. This is true of IA, given the global information space within which most organisations are interacting - be it where they work or where their data may reside and may thus need protecting (Holland, 2006).

3.8.4 **Cybernetics** was used as a backdrop in tracing the links from the original usage of cyber through to IG, as part of the historical research to reinterpret the meaning and contribution of IA to the InfoSoc.

3.8.5 **Bifurcation** had a relevance to this research (Luo, 1997) as many of the sources studied utilised definitions and constructs for InfoSec rather than IA. The Grounded Theory and new framework formulation were intended to articulate implications for change and new directions as a result of revisiting definitions and ensuring that these are more widely understood and accepted.

3.8.6 **Sensitivity** was also of importance as IA has been affected by the political and economic climate. There are three types of sensitivity identified in research – historical, political and contextual. Historical sensitivity aids understanding of governance of structures and situations (Silverman, 2009). Sensitivity to initial conditions is sometimes referred to as the "butterfly effect" and this is often how IA policy has been cascaded from central government outwards and downwards across the rest of the public sector and local government. Sensitivity is also raised with regard to the researcher being immersed in the subject area.

3.8.7 **Critical theory** is a theoretical approach that is sensitive to application. The speed of development of the InfoSoc and the technology that supports this, along with the shift in the political landscape in the UK in 2009, led to change in IS management radiating out from central government. Cognisance of this was important to the outcome of the research.

3.9 Ethics

> *"Ethics of research refers to assumptions about the responsibility of a researcher for the consequences of his/her research approach and its results"* (Iivari, *et al*., 1998, p.175).

3.9.1 This research involved sending surveys to IA practitioners and thus humans were objects of analysis (Vinson and Singer, 2001). Confidentiality for individuals was guaranteed with all personal identifiers eliminated, the data being presented anonymously. These

measures ensured that extracting individual identities was simply not possible. Another ethical aspect of the research was the decisions made with regard to the implications of the value-drive and action-effects of the inquiry identified by Wadsworth (1998) as the effects of: i) raising some questions and not others; ii) the effects of involving some people in the process and not others; iii) observing some phenomena and not others; iv) making this sense of it and not alternative senses; and deciding to take this action (or 'no' action) as a result of it rather than any other action etc.

3.9.2 As required by the research study regulations, the University of Wolverhampton Ethics Board provided ethical approval for the Survey Questionnaire both in 2010 and again in 2012.

3.10 Conclusions

3.10.1 The research was grounded in a historical content analysis of primary and secondary documentary sources to contextualise available IA concepts, doctrine, policies, procedures, and education in order to review how IA understanding evolved.

3.10.2 There are basic beliefs that define a particular research paradigm which must be supported by both an *epistemological* question – e.g. what is the basic belief about knowledge (in this instance, what can be known about IA) and a *methodological* question that describes how the researcher goes about finding out whatever can be known (Guba and Lincoln, 1994). This research used an exploratory (qualitative) survey method to obtain empirical evidence of both theoretical and practical IA understanding and to verify this against available

academic and practitioner outputs. The purpose was to learn from the experience of the surveyed target group and to validate the findings from the Literature Review.

3.10.3 Validation occurred through mixed method research utilising survey questionnaires, interviews and recording of observation through PAR case studies and reflexive ethnography to understand IA ontology and to interpret IA implementation in the context of the IA professionalism agenda. Through the Hegelian process of dialectical reasoning and the subsequent constructivist, inductive Grounded Theory work, the new meta framework - i3GRC™ – was realised.

Part 2 - Research

In this part, based on the research questions, the design of the questionnaire is developed and the appropriate target group is selected.

The survey execution, responses and interview analysis and the resultant survey findings are critically discussed utilising the identified themes throughout

4 RESEARCH FINDINGS AND DISCUSSION

4.1 Approach and Goals

4.1.1 As discussed in the Methodology Chapter, the researcher used mixed methods including an exploratory (qualitative) survey, freeform interviews and conducted two PAR case studies. The Questionnaires are represented in **Appendix I, Section 10.14** and **Section 10.15**.

4.1.2 The survey collection was supported by freeform interviews which were undertaken in person, face-to-face; by telephone; by Skype and via email leading to more consistent interpretation of the questions posed than standardized interviewing, particularly when respondents' situations are atypical (Conrad and Schober, 1999a/b). It was important to ensure that there was a shared doctrine attached to words so that the question asked was the one that was understood. No predetermined questions were asked, in order to remain as open and adaptable as possible to the interviewee's nature and priorities.

4.1.3 The researcher engaged in two extensive case studies, one in a large UK public sector local government environment from 2009 to 2011 and another in a global private sector services environment from 2011 to 2015. The description of the background of each Case Study environment and supporting materials have been placed in **Appendix II** in order to maintain the narrative style of this findings chapter. In particular, see **Section 11.1** and **Table 30**. The Public Sector Case Study is signposted throughout as **CS1** and the Private Sector Case Study is signposted as **CS2**.

4.1.4 The task of the survey, interview and case study research was to establish from practitioners the depth of IA understanding, having identified clear distinction in definitional terms between InfoSec and IA in the Literature Review. The results of the interviews added to the richness of the findings. In particular, a number of individuals took extra care in the provision of detail, which is captured in the detailed respondent memos produced in tabular format in **Appendix I, Section 10.17**. Together with the survey results, they contributed to the knowledge of IA understanding; implementation abilities of those actively engaged in the industry; helping to identify key themes to be incorporated into the future development of IA education and professionalisation. These themes influenced the Grounded Theory formulation. Subsequent sections of this chapter step through the responses and case study interactions, providing corresponding evidence, in a narrative style.

4.1.5 The goal of the research was to obtain empirical data regarding the level of IA practitioner understanding in order to provide evidence of the likely ability to achieve the stated goals of the UK Cyber Security Strategy. The intended outcomes were: i) to validate the findings of the Literature Review; ii) to provide IA practitioners with initiatives within which to frame the profession for the future, founded on historical underpinnings; and iii) to formulate a related Grounded Theory.

4.2 Target Groups and Research Execution

4.2.1 The questions were designed based on an assumption that the meaning of them would be commonly shared, the terms understood – and, if not, that this in itself would be raised as a finding to be addressed in the research. The survey question style followed University guidelines.

4.2.2 The first group was made up of industry experts from IAAC, representing a cross-section of both InfoSec and IA professionals of varying lengths of service in public and private sectors, third sector and academia, with differing certifications, education and levels of understanding, as well as membership of several worldwide industry bodies (ISACA, (ISC)², ISSA, IAAC, BCS, IISP etc), largely all members of IAAC. The second circulation group was made up of mainly operational Security Officers, across multiple geographies (spanning US, Europe, and Asia) and industry sectors – in order to understand the challenges of those in the role of day-to-day practitioner [**CS2**]. Further participant details are provided in **Table 20, Appendix I** at **Section 10.16**. Studying a population by studying a presentative sample is a known best practice in statistical inference analysis. The population was made up of several units from which the research could observe characteristics and draw samples for analysis. A sample size of greater than 30 is considered sufficient reference material for qualitative analysis. This sample size is therefore considered to be sufficient.

4.2.3 Figure 28 shows the spread where I is the IAAC circulation, O is Other and P is the Private Sector Outsourcing circulation.

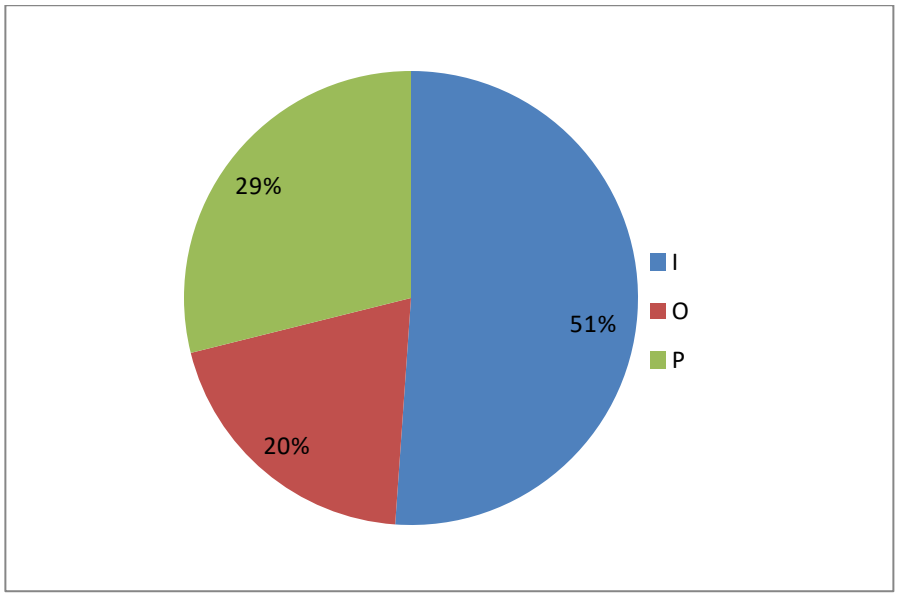


Figure 28: Total Survey Types

4.2.4 Respondent Demographics are depicted in Figure 29 below:

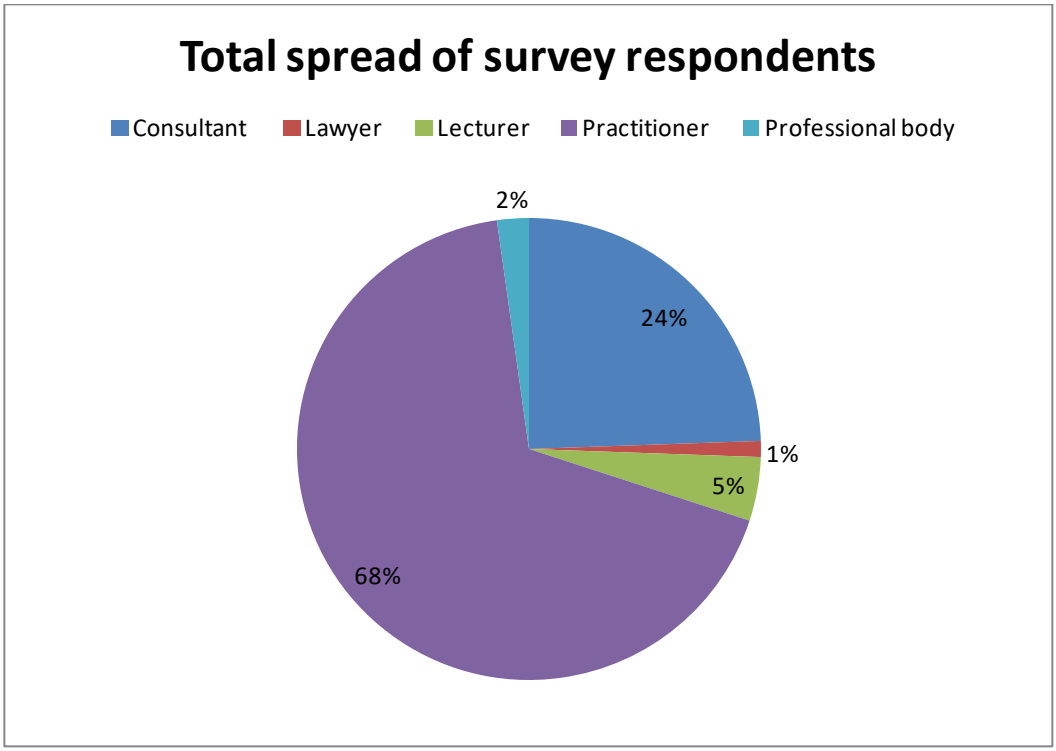


Figure 29: Total Spread of Respondents

4.2.5 As different security and data protection legislation applies in each geographic region, the purpose of increasing the scope of the survey was to investigate to what extent, and how, operating in different environments affects cultural awareness and understanding amongst practitioners. Figure 30 below identifies the geographical spread of respondents.

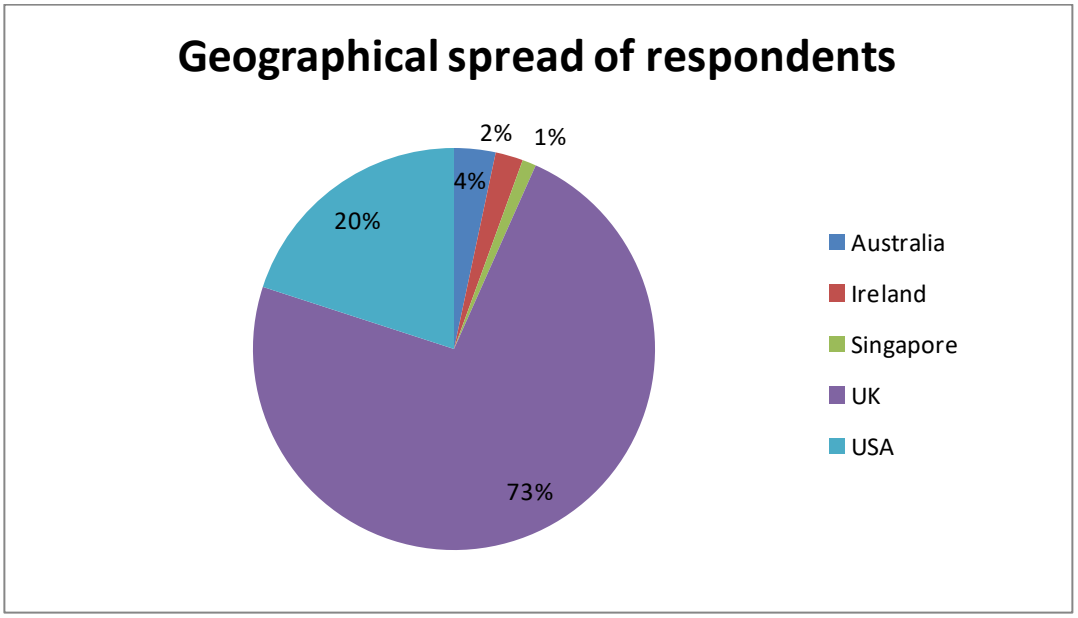


Figure 30: Geographical Spread of Respondents

4.3 Data Collection and Analysis

4.3.1 In order to obtain further knowledge, verify thinking and increase the validity of the research, a number of unstructured, informal, freeform, conversational and discursive interviews were conducted with subject matter experts, including senior IA practitioners.

4.3.2 The researcher is a member of a number of UK industry groups which afforded easy access to IA practitioners and InfoSec professionals – many of whom cross over and are represented in each group.

Removal of duplication of responses was part of the data analysis process. The results are reflected in these findings.

4.3.3 Figure 31 identifies the activities undertaken in order to ensure participation within the chosen target groups and gather adequate data collection for analysis and validation purposes.

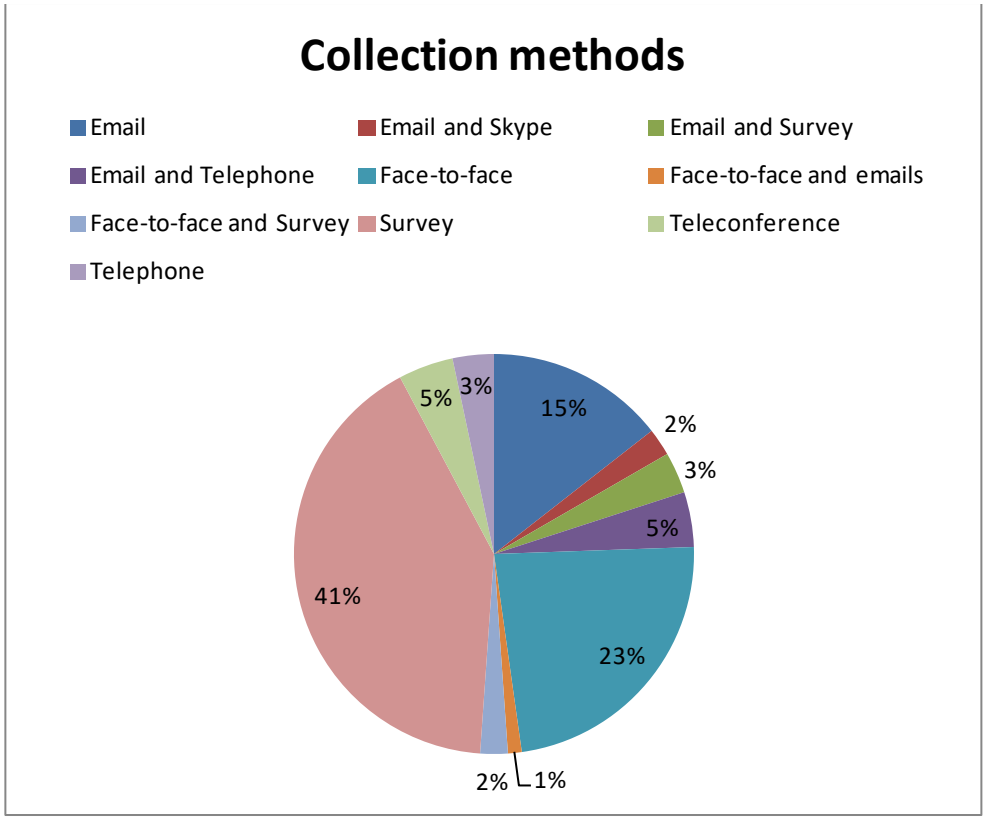


Figure 31: Collection Methods Utilisation

4.3.4 Coding for the respondents is provided in **Appendix I**, before **Table 20** and is signposted throughout the rest of Chapters 4 and 5 by way of brackets, bold number and letter configurations based on the codes listed in **Table 5** below. Thus **[11E]** refers to a UK legal expert when cross referenced with **Table 20**.

Code	Description of interaction / methodology
E	Email correspondence
ES	Survey respondent with extra email input and conversational follow-up
ESk	Emails and Skype semi-structured interview
ET	Email and telephone
F	Face-to-Face semi-structured interview
FE	Face-to-Face semi-structured interview and email follow-up
FS	Face-to-Face semi-structured interview and survey completion
S	Survey respondent
T	Telephone semi-structured interview
Te	Teleconference with global private sector clients, i3GRC™ explained

Table 5: Respondent Coding

4.4 Validation Methods

4.4.1 Triangulation methods were used to validate the observations and identify biases in the data gathered, as depicted in Figure 32 below.

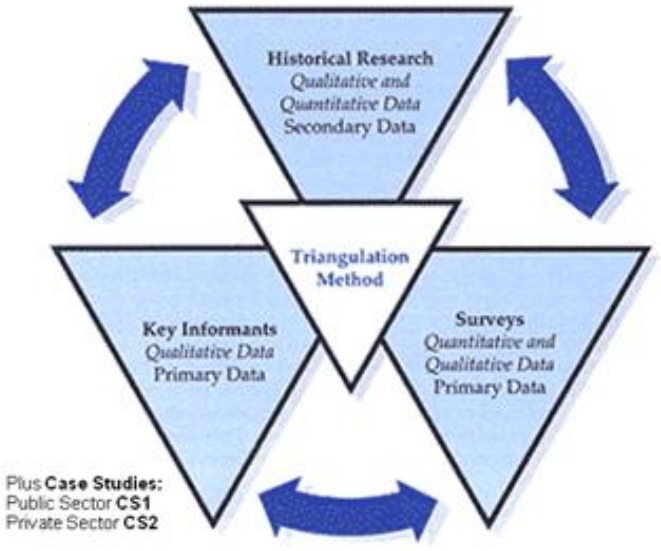


Figure 32: Data Triangulation

4.4.2 Triangulation is the exercise of using more than one method to collect data on the same topic. This ensures data correlation and validation occurs. Triangulation has taken the following forms: i) comparison and correlation of the survey results, the interviews, and the public and private sector Case Studies [**CS1** and **CS2**, see **Table 6**], one to another; ii) comparison with other theses including Richardson (2012) and Cherdantseva (2014), which has been vital; and iii) comparison with the available academic research and the outputs of various government bodies and resources available to the community of practitioners.

4.4.3 The results of the questionnaires were used to both answer the research questions and to test and validate empirical generalisations which were formed throughout the theory building process, in order to identify common relationships across them and to provide statements about the object of study (Gable, 1994, p.114).

4.4.4 The method provides only a "snapshot" of the actual situation and does not necessarily allow understanding of the underlying meaning of gathered data. The benefits of the researcher's own experience and the PAR carried out helped to enrich these findings.

4.4.5 As the bulk of the data collection was gathered through the historical research phase, this became the pivotal point of the triangulation activities. Consistently throughout the research, the views of known and available expert practitioners in the industry have been sought in order to ground the theory being developed. These experts are part of the IAAC community originally surveyed. The interview (key

informants) and survey data were combined in the memo writing for the Grounded Theory building.

4.4.6 Ongoing literature searches were carried out in parallel with the ethnographic study, alongside PAR observations which were made by interviewing multiple stakeholders at different levels in various organisations. Iterative qualitative content analysis was then performed against the identified themes. Reviews took place internally within each CS organisation, not externally, in order to prevent skew. All available and applicable Internal Audit and external resource reports were reviewed as part of the data gathering and triangulation in order to ensure the theory being built addressed the identified gaps.

4.4.7 The process was a reflective one. Further validation was achieved through reflexive discussion with each organisation; the findings have been fed back to various professional peer audiences. A number of conferences, seminars, and workshops were also attended where the work was presented in a style conducive to discourse so that shared views and understanding could be captured. Posters were also prepared and presented at several events. See **Appendix I**, **Section 10.2**.

4.5 Case Studies

4.5.1 During the span of the research study, two significant periods of time were spent; one in a large UK public sector local council [**CS1**] and one in a large global private sector outsourcing business [**CS2**], the names of neither are being explicitly disclosed in order to maintain confidentiality.

4.5.2 Table 6 below provides a comparison of **CS1** and **CS2** organisational approaches to IA implementation, highlighting both the similarities as well as the differences across the identified survey themes.

Areas	Public Sector [CS1]	Private Sector [CS2
Timeline	2008-2010	2011-2015
Employees	c.13,000	107,000
Terminology	InfoSec centric – no adoption of the UK IA language change(s)	GR**C** Heavy emphasis on **Compliance**
Drivers and Obligations	GCSx Code of Connection (CoCo) – no connection = no system connectivity! UK Government obligation, resisted for as long as possible!	PCI DSS for retail and commercial HIPAA for US Healthcare ISO 27001 global certification Cloud Security Alliance CSTAR for Cloud Services NIST, FISMA, SANS, ISAE 3402
Standards and Measurements	ISO 27001 accepted as a framework worthy of consideration but not vital HMG Security Policy Framework IAMM – considered through the PAR process	ISO 27001 global certification being sought for all Data Centres – heavy requirement and expectation from worldwide global customers Significant measurement from external audits imposed by client companies
Impact of culture and politics	Under Lib Dem control at the time of AR – this had a notable impact on budget and focus ICT very hands off in terms of people engagement across the organisation – "the department of *no*".....*No real skills with regard to speaking to leadership regarding InfoSec risks and the UK Government IA requirements.*	Different country by country impacts experienced but more particularly in the outsourcing dynamic, where the cultural impact of employees not adhering to security policy control implementation was being increasingly felt as a result executive leadership decisions to focus on growing business in certain locations.
Professionalism of ICT and IA	No initial focus but the researcher was able to positively influence those worked with to follow careers in the security industry, to take up membership of relevant professional bodies and to share knowledge and learning more positively. Delivered InfoSec Awareness sessions to thousands of Council employees and did outreach presentations to schools and other groups to ensure positive engagement and consistency of messaging.	Stealth newsletter started in 2012 which by 2015 had thousands of recipients worldwide, 15th of every month, delivered to their Inbox highlighting why the controls were relevant, which news stories were of corresponding value to learn from and what the development focus for the GRC programme was. The researcher mentored a number of individuals, ensuring their skills were improved and sustainable.
Information Society	Not applicable at the time – although medical monitoring devices in the homes of the elderly or bewildered were already being considered from a security and data protection perspective.	Multiple issues for multiple different clients globally but the GRC programme was not specifically impacted as the focus was on internal signal reporting.
Barriers	Austerity as a result of the financial crash.	Ongoing business attrition, loss of key employees through ongoing job losses.

Table 6: Case Study Comparison

4.5.3 In **CS1**, the researcher was in the position of that of an external IA consultant. There are many independent consultants in the industry, worldwide. **CS1** involved the roll-out of a government mandated organisation wide IA compliance management programme which included the delivery of InfoSec Awareness programme, in person, to hundreds of employees across a region of the UK. The PAR resulted in the publication of an Information Security Manager's guide book (Simmons, 2012a) representing a compilation of learning and sharing of practical lessons learnt.

4.5.4 In **CS2**, the researcher had changed function to that of a permanent senior global focus for a large IT outsourcing company, initially with a specific security policy related improvement task. **CS2** resulted in the creation of a Unified Compliance Framework (UCF) through mature implementation of GRC technology across a multi-industry, all sector landscape. The global organisational reach afforded the researcher the opportunity to engage with a wide selection of respondents, reflected in the survey and interview data, representing multiple disciplines. The case studies provide explanation of the observed phenomena and demonstrate understanding of the subject of the investigation in its context and environment. The results of the case studies have both corroborated and enhanced the survey results. Sector comparison has also assisted the formulation of the theoretical conjecture and confirmation of hypotheses.

4.5.5 In **CS2**, the researcher had the opportunity to create observations of deliberate intervention, bringing about change through the delivery of dependent variables of global communication in a private sector setting. In **CS2** (see **Appendix II, Section 11.2** and **11.3**), HEART was utilised as a communication tool to signify that what was designed for the benefit of all was a **H**olistic **E**nterprise **A**ssurance **R**isk and **T**rust framework.

4.5.6 In **CS2**, the GRC-related entity was buried organisationally within a sub-entity of the entity being assessed/audited, which did not provide the appropriate separation of duties nor afford the board the ability to benefit from accurate independent assurance. As a technology company, and in keeping with its competitors, it had no incentive to consider the more strategic elements of GRC implementation, beyond the available technology solution – a solution to a problem largely exacerbated by technology. The researcher provided an IG Strategy framework within which to manage information within the context of the most pressing legislative and compliance requirements. Internal controls required rethinking, reprioritising and risk management in order to shift from the initial narrow focus on "tick box" assessments to a more multidisciplinary approach, with results sharing and improvement plans in place as continual audit evidence.

4.5.7 Gillon *et al.* (2011) identified the need to do organisational focussed research and this case study embraced the requirement. By the nature of the private sector case study, the researcher had to take an "outside in" view in order to ensure cognizance of and communication

with the client (customer) stakeholders on an ongoing basis. This is represented in the pictorial at Figure 33 below.

Figure 33: IG Stakeholders, Source: Forrester (2015)

4.6 Terminology

4.6.1 The first section of the survey was designed to gauge depth of IA understanding of the respondents and to ascertain any temporal change. See Memos at **Appendix I, Section 10.17, Table 21**. Together with the extensive Literature Review, this section answers the first research question: *Can professional IA practice be improved through enhanced IA understanding?*

4.6.2 Senior practitioners had known about both the distinction (between InfoSec and IA) and the definitions for over 30 years. **[16FS, 61FS]** with 2010 being the most recent. **[72S]** The terms were consistently

used interchangeably, as was found in the Literature Review. **[31ES, 45S, 49S, 50S, 54S, 66S, 69S, 71S, 75S, 76S, 78S**] though one respondent stated IA was "undefined with multiple meanings". **[67S**]

4.6.3 In the PAR, there was evidence of the difference between what IA means and what people are actually doing – in terms of its constituent parts - to achieve it [**CS1**, **CS2**]. As identified in the Literature Review, individuals have professional identities. A security person will describe IT Governance in InfoSec and ISO 27001 terms and frame of reference. **[35F]** An Information and Records Management (IRM) person describes the IG space with a different emphasis on the locus of terminology. **[25E]** An IT person will often describe their ontology in IT Infrastructure Library (ITIL) terms. **[59S]** There is a difference in terminology usage across the world. The term IA is not widely used in South East Asia. One respondent specifically stated that "Assurance has an interesting perception in many languages and cultures and in Australia it hasn't really taken off because many people consider it to be a bit of a buzzword that has no real defined meaning – which is an important requirement when trying to win over important stakeholders in an ISP". **[48S, 57S]**

4.6.4 According to respondents, there is a lack of related legal oversight in Australia and in the Asia Pacific region, outside of specific government requirements and some weak privacy legislation. **[57E, 58S]**

4.6.5 The word cloud at Figure 34 represents the **Terminology** findings:

Figure 34: Word Cloud created 12 September 2015

4.6.6 Many other terms were referenced, identified in the list below:

Information Protection;
Data Classification and Management;
Data Protection;
Cybersecurity;
InfoSec;
Accessibility;
Corporate Security Governance;
Global security policies;
IRM;
Minimalist compliant;
Protection of IT assets;
Level of trust;
Lessen or eliminate related vulnerabilities;
Corporate Security Governance;
Security risk and compliance planning;
Build the confidence in the stakeholders;
Risk management programme (identification, evaluation, treatment of risks);
IX = Information Exploitation.

4.6.7 Information Exploitation was a term identified by UK MoD respondents. **[10FS, 14F]**

4.6.8 When an audience of members of the BCS Information Risk Management and Assurance (IRMA) group were asked to come up

with words or phrases to describe IA the following terms were used [**Appendix I**, presentation reference **10.2.4**]: Quality and accuracy; Reliability; Reputation; Compliance; Do it correctly; "I know it when I see it!"; CESG Standards.

4.6.9 Whilst this used to be the IRM and *Audit* Group (IRMA), it was clear that despite the change to the IRM and *Assurance* labelling, there was little real IA understanding, where it comes from and what skills are needed to effectively implement it. The group were, in 2010, considering changing to an IG label given the focus on Governance within the Corporate, Financial and Health sectors, though at the time of submission this change had still not taken place.

4.6.10 In conversation, many practitioners believed that it was "just something that CESG threw into the mix in the mid noughties". **[69S, 78S]** The responses were invariably subjective.

4.6.11 As a term, IA was considered useful to industry specialists only as a term for discussion amongst each other, whereas, for example, the use of "cyber" as a label was believed to have gained better traction and garnered wider interest and adoption amongst business leaders, government and industry alike. **[1F]**

4.6.12 Only one respondent **[52S]** identified the evolution previously presented in Figure 24 (page 98) - *Security > IT Security > Information Security > Information Assurance > GRC - It is an evolution*. **[52S]**, (December 2012).

4.6.13 Similarly, only one respondent **[58S]** highlighted that appropriate implementation of monitoring and reporting tools is a first major step.

However, several respondents did identify that IA is but one *part* of IG, requiring greater organisational governance. **[15ES, 53S, 54S, 58S, 60S, 68S, 71S, 77S, 81S]** Respondent **60S** phrased it thus: "IA is about managing the quality and security of information. It is one part of IG".

4.6.14 Respondent **[65S]** identified that the use of acronyms in the spoken word, as opposed to the written word, had led to confusion and misunderstanding.

4.6.15 In both **CS1** and **CS2**, the researcher observed many examples of misunderstood sets of terminology and the implications this is causing within the community. Contracts were being signed up to on the premise that a service provider would "be compliant with PCI", without all parties understanding the implications of what that meant. When something goes wrong, unravelling responsibilities and actions to be taken becomes cumbersome and costly. Respondents identified this need for IA professionals to be well versed in legal and contractual language in order to best serve their organisations in their roles. **[46S, 53S, 69S]**

4.6.16 There are cost implications which have to be understood, based on the services selected for contractual delivery, and those that are left out. Financial understanding is another aspect to the skills and competency portfolio of an IA professional, an area that is not part of any current educational framework. Errors of omission in contractual language can have discernible impact on both the operation of

services and the costs incurred by the business. **[7ES, 10FS, 14F, 56S, 57S, 59S, 65S, 67S, 50S, 78S, 79S]**

4.6.17 In the private sector case study [**CS2**], the researcher witnessed a global IT outsourcing company with lawyers still utilising contractual language referring to the backup of data to floppy disk. Nobody had taken the time to update this content and address obvious gaps in terminology despite the contractual implications.

4.6.18 Exception Management is another example of a misunderstood concept. In the private sector case study, exceptions to security policy were being consistently treated as risks, which was not always the case. **[CS2]** An exception against policy was raised for every instance of not adhering to policy, even if the lack of adherence was actually an instance of the provision of security *greater* than that required by the original baseline.

4.6.19 Other examples include Governance, often too broad in its usage but intended to mean Control and Authority – largely in business terms. *Demand* in German is the word used to ask for something; there is no tone intended. A common understanding of terminology is vital given that, with outsourcing and off shoring, the native language of those required to take action may not be English. **[83F]**

4.6.20 Many programmes of work may take several years and then they are out of date for the next project. Seeking to overlay IA requirements is always difficult, given that it ultimately needs to be built into the framework of operation from the outset. **[7ES, 46S, 47S, 49S, 50S, 58S]**

4.6.21 There is frequent mixing of concepts and the confusion is leading to difficulty in selling IA to Board level or effectively implementing it. **[62S, 69S]** From the survey responses, Table 7 presents a list of words identified as ones that matter most and least to IA practitioners:

Words that matter most	**Words that matter least**
Trust	Security
Accountability	Best Practice
Dependence	"we've always done it this way"
Authentication	Guarantee
Non-repudiation	Certainty
Enabling	
Safety	
Protection	
Teaming	
Integration	
Concurrency	
Probability	
Risk	

Table 7: Words Matter

4.6.22 This presents challenges for future development of InfoSec Awareness materials, or cybersecurity related awareness campaigns, but also offers options for change in the prevailing dialogue and rhetoric usage. Also, the researcher observed a distinction between the public and private sector understanding of the terminology in use.

4.7 Drivers and Obligations

4.7.1 The second section of the survey was designed to elicit understanding with regard to drivers and obligations for implementing IA programmes. See Memos at **Appendix I, Section 10.17, Table 22**.

4.7.2 The findings bore out understanding of benefits and returns to be appreciated from creating a corporate IA culture and programme, also identified in the Literature Review. Respondents identified benefits including improved IM; more effective use of ICT; resilient ICT; better business continuity planning and greater security to operations and to business, as well as for individuals. **[10FS]**

4.7.3 Respondents **[10FS, 14F, 45S, 46S, 47S, 48S, 50S, 56S, 59S, 65S, 67S, 72S, 74S, 76S, 78S]** concurred that the risks of neglecting this aspect of corporate governance might include: i) higher operating costs, including both daily costs due to inadequacies of the information infrastructure (e.g. from poor records management) and irregular costs due to major incidents or adverse events; ii) greater uncertainty in forecasting and planning future costs; and iii) more difficult and less beneficial relationships with partners etc.

4.7.4 In the UK, the public sector focus has been on compliance as a result of government IA frameworks, data protection legislation requirements and the IAMM. The latter was cited as the reference point for prioritisation, with many bodies required to achieve Level 3. **[10FS, 14F, 76S]**

4.7.5 Respondents concurred with the Literature Review findings that fear was driving compliance activities. **[48S, 52S]** The private sector IA

focus has been on financial sector regulation, through "know your customer (KYC)" programmes. **[46S, 52S, 53S, 60S]** Operational Risk has not been fully addressed.

4.7.6 One respondent stated *"*Public sector organisations that I encounter take no constructive notice until hit by the ICO – even then they are not fully embracing the requirements. Private sector tries much harder but is prepared to take risks.*"* **[15ES]**

> *Yesterday I heard a comment that the difference between "InfoSec" and "IA" is that between the private and public sectors. The more I think on it, the more interesting the comment becomes.* *Anecdote provided by third party, 12 November 2010, 7ES*

4.7.7 There were respondents who believed that the academic and third sectors are laggards in IA. **[52S, 65S]** In particular, one respondent specifically fed back: "I don't think academics know what any of these terms mean.... In general, academia seems pretty rubbish" **[75S]** Others believed that the public sector and academia were ahead. **[58S]** Still other respondents **[46S, 63S, 75S]** believed that the manufacturing sector were laggards.

4.7.8 Respondent **73S** identified that "Academics are not providing enough good research (but that's because there is little funding available) and need to become more 'business-centric'*"*. However, respondent **58S** believed that "public/academic sectors are well ahead of many private institutions". These divided opinions are not unusual across sectors on the premise of a belief that each sector is doing better or worse than the other – until an individual changes job or function within a different sector and sees the reality for themselves.

4.7.9 Research by the IISP showed the extent of the divided opinions with there being little gap between those who felt there was improvement in the ability to defend systems and those who were neutral on the subject (IISP, 2016).

4.7.10 The insurance question was asked in order to assess maturity level in terms of adoption of this mitigation strategy. The cost of implementing best practices in IA may well be more than any reduction in insurance premiums. **[46S, 47S]** It comes down to return on investment of implementing best practices with the reduction in insurance premiums being an added benefit. Another aspect identified was that of the problem of how best to arrange accreditation, to the extent that the insurance companies would accept evidence of compliance. A regular audit was the normal approach, but the costs of undertaking this cannot be ignored. A self-audit runs the risk of becoming a tick-in-the-box exercise that will not benefit 'the customer' until the company has been found guilty of a violation. **[7ES, 73S]** This does not address the public sector, which holds an appreciable amount of information and does not insure their services as, by their nature, they are government backed and do not need to do so. The research continued to identify wicked problems without solutions.

4.7.11 PAR **[CS2]** identified that elements of insurance require further consideration, represented in Table 8 below, with a view to changing the focus of the rhetoric from a budget model to a turnover model.

Required	Impediments
People	Personalities
Process	Costs
Technology	Maturity

Table 8: Considerations for Insurance/Under writing industry rethink

4.7.12 Professionals identified a need to have broader education in finance models in order to present risk effectively to management and leadership, in compelling business terms. **[56S, 76S]** Practitioners cannot be in a position of raising the identification of risks to management without the ability to understand the financial implications of implementation of risk reduction strategies.

4.8 Standards and Measurements

4.8.1 IA has been making the transition from a technical activity to a senior management and board issue for several decades. Following on from Section 4.7, this next section was designed to elicit mechanisms for measuring the effectiveness of IA implementation on the premise that for many senior managers, what gets measured, gets managed, and vice versa. See Memos at **Appendix I, Section 10.17, Table 23**.

4.8.2 PAR [**CS2**] identified that in the service provision sector had been told not to say "best practice" anymore as the implication of legal interpretation of the terminology could result in a law suit for not achieving perfection. In fact, for some, the term "best practice" was deemed too emotive and context dependent. However, as one respondent identified "The divergence between good practice and common practice is still far too wide". **[74S]**

4.8.3 ISO 27001 was the most quoted standard by multiple respondents. **[10FS, 46S, 48S, 68S, 71S]** Implementation of ISO 27001 is accepted as best practice. However, it cannot be prescriptive because technology is changing so quickly. ISO 27001 is *not* an IA standard; it is an InfoSec management standard. There is no IA standard; nor is there a globally accepted cybersecurity standard. A list of identified related standards and Best Practices available to address InfoSec and management, equally identified by other researchers, has been reproduced in **Appendix I**, **Section 10.19**.

4.8.4 From the private sector point of view, whether IA is achieved or not is measured against the business attributes that are specified and agreed as a requirement by the customer/client. The benefits are subsequently measured in terms of the degree to which the fulfilment of a customer/client requirement supports, lends support or advances the aims, goals, and mission of the customer/client, whether financially or otherwise. **[47S]**

4.8.5 The same key issues continue to arise through audits and reviews, identified by many professionals ((ISC)², 2013a) and respondents alike **[51S**, **68S]**: i) incorrect access rights (account); ii) no systematic responsibility for accesses (account); iii) who did what, when (also known as segregation of duty); iv) lacking corrective actions/follow-up (management); v) lacking documentation of decisions (management); and vi) faulty code, patching, or non-best practice (management).

4.8.6 One respondent **[57S]** articulated the following overall programme approach, consistently understood by the majority of respondents and experienced by the researcher in **CS2**. Those elements in **bold** are intended to denote activities/processes to provide assurance to stakeholders.

- *Security Program Management*
  - *Planning (Strategy and Security Requirements, continual improvement)*
  - *Program Assessment, Gap Analysis*
    - *Security Governance*
      - *Policies, Processes and Procedures*
      - *Legal and Regulatory*
      - *Risk Management*
      - ***Review***
      - ***Enforcement /Compliance***
        - *Audit*
        - *Penetration Testing*
    - ***Security Technology and Architecture***
      - *Definitions, Design to comply with security requirements, Development and testing*
    - *Security Operations*
      - ***Compliance to Procedures***
      - *Risk Assessment*
      - *Implementation*
      - *Vulnerability Management*
      - *Patch Management*
      - *Incident Management*
      - *Event Management*
      - *Reporting*

4.8.7 The public sector expects the supply chain to be mature in terms of IA practice. However, contractual terms are inadequate and are not being policed. Without sufficient oversight and ability to evidence the required level of IP, further breaches are inevitable. **[50S]**

4.9 Impact of Culture and Politics

4.9.1 This area of focus arose out of several themes from the Literature Review analysis, including organisational and geographical political context. See Memos at **Appendix I, Section 10.17, Table 24**. The UK Labour government went through an extensive transformational agenda during the first part of the new millennium. In May 2009, the change from a Labour to a coalition led government created a shift in focus, following a significant period of activity implementing the Data Handling Review requirements. This is highlighted in the **IA Chronology, Appendix III**. The questions for consideration in this section therefore focussed on whether change in political landscape might change priorities and thus change resource allocation. The findings bore out this reality in parts of the public sector, and also in the private sector servicing the public sector.

4.9.2 The research was undertaken at a time when changes in culture were evident as a result of the terrorist attacks in the US on 11 September 2001 and the actions of Wikileaks and Edward Snowden, aspects borne out specifically by survey respondents. **[48S, 51S, 58S]**

4.9.3 The rhetoric is different in the ICT and Security trade press. **[15ES]** The IT industry is not as mature as other regulated industries. Self-regulation has not been universally adopted. **[7ES, 15ES]** Respondents noted that private sector organisations that provide outsourced services to the UK public sector were more closely monitored by business leaders, though the requests to meet standards came with cost implications. **[7ES, 24T, 54S]**

4.9.4 Promoting IA expertise was only going to make a difference if the whole of the target audience was alert to the benefits and the necessity of change, and if the organisation being served also had embedded within it a number of leaders able to take the rest of the teams along with them. If an organisation's management are unwilling to adapt, it was only ever going to be difficult to trigger the required cultural change. **[15ES]**

4.9.5 2010 was a particularly active year in terms of the design of the UK Government's IA professionalism agenda. The UK Government had an active role in the landscape, as expressed by one respondent: "not just regulation, but monitoring and enforcing due process and providing the right incentives and disincentives". **[7ES, 11E]**

4.9.6 Respondents identified that the Public Sector had become more attuned to the need for InfoSec with more emphasis on this area which, at minimum, improves awareness. **[1F, 7ES, 10FS, 15ES, 31ES, 49S, 60S, 79S]** However, additional awareness or investment in resources into security measures does not automatically equate to better security or better IP (Kaplan, 2008).

4.9.7 There is an ethical dimension to striking the balance between the effective implementation of operational security (across an organisational horizontal) against the Private Sector (team) need to see an ongoing increase in sales of Security Services (along the outsourcing vertical), whether relevant or required. **[48S, 56S]**

4.9.8 One respondent stated that IA *was* InfoSec but was changed to reflect the demands of the UK public sector. **[49S]** The Literature Review identified how the usage of the terminology was borne out of government led initiatives. In 2010, the complexity of the existing UK public sector landscape was clear given the number of different bodies with competing agendas – MoD, Serious Organised Crime Agency (SOCA at the time, now National Crime Agency [NCA]), MI5, MI6, GCHQ, eCrime Units, Criminal Asset Recovery Unit, Office of CyberSecurity, CyberSecurity Operations Centre, expanded Special Forces and more. **[10FS, 14F]**

4.9.9 Historically, fraud prevention has been carried out as a separate activity from cybercrime, at a policing level, and the same can be said for organisational implementation. This has been wasteful of resources and lacks a combination of available intelligence. There are a number of industry, government and law enforcement fraud intelligence assessments which are not brought together to give one common, authoritative picture. Given that the criminals are using cyberspace as the medium through which they are committing fraud, the correlation between fraud and cybercrime was only fully realised in 2015 with the first release of co-ordinated crime statistics reporting. **[5F]** It was also clear that improved coordination of the multiplicity of different organisations would be required. For one respondent, it was hoped that perhaps by 2015 there would be a Department of Information and Infrastructure, though there is still no sign of this yet (2017). **[5F]**

4.9.10 Passionate leadership carries little physical cost to the organisation yet it can have huge impact. This explains why organisations with limited resources can make appreciable improvements. The overriding sense from respondents was that the task was not mission impossible, rather it was mission critical. **[10FS, 15ES]** However, the power of one enthusiast may be insufficient depending on the size of organisation and the volume of information records requiring protection. Quality, compliance and IP are an outcome of what is done; they are not *in addition* to what is done – by all employees. **[60S, 75S]**

4.9.11 The historical anecdote below is shared as evidence of how long the repeated issues have been experienced and how important the "tone at the top" is to the success of any change management undertaking.

> *Cement Ltd, 1967*
>
> *A new HR system was being implemented. The staff were worried about IT having access to their personnel data, including their salaries as this would be the first time all of that information would be in the one, accessible place.*
>
> *The then MD took the bold step of putting his salary on an A4 sheet of paper, poster style, on the main reception notice board stating what he was getting paid, on the premise of being confident that he was worth it. The message to all of his employees was this – if you are paid too little, the company should be embarrassed; if you are paid too much, either you should be embarrassed or you need to work harder to justify the salary!*
>
> *Leadership made the significant difference to the ultimate success of the implementation of this new system as everyone got on with allowing their data to be input into it.*
>
> (Anecdote provided by respondent **22F**)

4.10 Professionalism of IA

4.10.1 This area of study was designed to elicit understanding of the impact of the IA professionalism agenda *at the time of the research*. See Memos at **Appendix I, Section 10.17, Table 25**. Combined with the Literature Review, this section answers the second research question(s): How has the extensive body of knowledge influenced professionals?

4.10.2 Overall, the belief amongst respondents is that IA has not achieved the status of a profession. **[3F, 5F, 10FS, 14F]** The researcher contends that the ongoing confusion in terminology is not aiding progress, leading to question whether we seeking to professionalise "cyber professionals", "InfoSec professionals" or "IA professionals". If the latter, then there is no representative IA membership body for them to belong to.

4.10.3 The existence of a NIAS since 2003 helped to increase IA understanding but respondents felt that it lacked political momentum. In professionalising the industry, positively there is a greater presence of security experienced C-level executives at the top of organisations that are discussing and adding IA to their strategies. Professionalising the industry has created a greater drive for minimum standards, baselines, benchmarks and levels of compliance that must be met, to ensure that any organisation is not impacted by a lack of adherence to local laws and regulatory requirements. For many, there is clear budget and strategy for security risk and compliance planning, delivering IA. There is greater awareness of the threat landscape and

improved appetite to understand the risk posture of organisations. Managed risk brings value to an organisation; poorly managed risks devalue an organisation. **[54S]**

4.10.4 The ongoing "skills crisis" rhetoric and the identified gaps ((ISC)², 2011d/2013a/2015g) were of concern to the researcher given the volume of available information, certification, standardisation, accreditation and professional membership bodies.

4.10.5 Many respondents believed that professionalism was a key strategic enabler. **[1F, 10FS, 15ES, 18E, 20F, 21E, 26F, 27E, 28T, 49S, 63S, 66S, 79S]** IA is not a core discipline in its own right, it is not academically accepted. **[20F]** There are IT bodies and InfoSec bodies. There is no IA professional membership body. Negatively, there is a belief that there is a large group of accredited professionals that appear to have achieved their qualifications without relevant experience, gaining senior level roles in organisations and damaging the credibility of IA as a result. Part of the risk lies with the recruiters not checking experience as well as accreditation (perhaps being ill informed and/or time poor) but also with the professional industry bodies not making the experience measurement process sufficiently robust. The gap is narrowing over time as the various membership bodies address it. **[48S]**

4.10.6 As was found in Section 4.11, management leadership and direction is vital. Many respondents identified concerns regarding a lack of leadership. **[10FS, 14F, 48S, 53S, 65S, 84F]** In the UK public sector, the Senior Information Risk Owner (SIRO) was designed to take on

the function that would help to filter these issues up, through and to – and to help the decision making processes. However, the nominated individuals, including the Heads of Profession, have historically not been from the InfoSec profession and thus lack grounding in the concepts and terminology. This, in itself, perpetuates unprofessionalism. **[10FS, 20F]** The Council for Professors and Heads of Computing (CPHC) help to advise the UK Government in managing this stream of professionals though there is a high turnover in Cabinet Office staff and there was no evidence that they had read the available reports. **[84F]**

4.10.7 This difficulty was also articulated by a peer group the researcher presented to [**Appendix I, 10.2.8**]. The views expressed were that any organisations Board of Directors needs to understand the threat independently of the employed professional(s), particularly if they turn to a professional for advice. However, if the professional is finding the subject area too complex to understand, the question then asked was – "who will they [the Board] trust to advise them on this complex subject?".

4.10.8 This situation is not specific to the public sector. Speaking at an open conference in December 2011, the CSO of BP was a self-confessed unqualified individual but expected his staff to gain relevant qualifications. One of the most senior figures in Security in BT has no discernible relevant qualifications or certifications, again self-confessed. This opens up the profession to direct challenge as to why

effort is applied to professionalising an industry when it does not employ accredited or certified individuals in senior roles.

4.10.9 Whilst a multiplicity of choice was identified by respondents – IISP, UK CESG, IAAC, BCS, IET, ISACA, (ISC)², ISSA, the Big Four, SANS, SABSA, BCS IRMA, IBM, ISF, Oracle, Tripwire, HP - the majority stated that they would turn to people they *knew*, as opposed to specific professional membership bodies, for advice and guidance. With so many membership bodies, consideration needs to be given as to how many of their members overlap and to what extent the volume is creating a dilution effect. However, this was not something the scope of research could encompass. One survey respondent expressed these challenges, represented below.

> *As long as each of these areas has societies where annual dues are payable, separate journals and, dare I say it, separate vested interests, the array of information/data/knowledge groups can never be viewed as a cohesive whole, no matter what academic studies may argue for it. There are economic reasons why merging and cohesiveness are desirable - not only for the work done in the field, but also the research work which is duplicated/unseen/misunderstood... And then there are the international differences: the US will never see things the British/European/Asian way, and vice versa...* (Email per comms, 8 September 2015)

4.10.10 The ethical dimension appeared regularly as a theme throughout this study. **[50S]** All the widely known professional membership bodies in

the ICT industry, and those specifically addressing InfoSec and IA have Codes of Ethics, requirements for annual continuous professional development (CPD), levels of competencies, assessments, etc. In spite of this, there was a call for a cybersecurity code of ethics or professional membership body (*in conversation, IAAC PDM, 8 September 2015, IISP Congress 2016).* **[28T]** The researcher believes that to do so would risk the development of new avenues for addressing an already solved problem and the dilution of the existing BoK. **[16FS, 45S, 47S]** This is not to say that the existing Codes of Ethics would not benefit from being updated.

4.10.11 Enforcement is also an issue - without threat of sanction by a professional body, no code of conduct or ethics can be considered to be effective. **[31ES, 57S]**. This changes behaviour, with an increase in security spending as well as a delay in being able to fill vacant positions due to a lack of available talent. The length of time to work through academia makes the process longer so more vocational training may be required. **[71S]**

4.10.12 (ISC)2, ISSA and BCS all operate a CPD approach. This supports the requirement to ensure that professional development processes exist in order to maintain the quality and relevance of professional services throughout a practitioner's working life. There are many IA practitioners who are dismissive of certifications provided by membership bodies. This does a disservice to those who take the time to invest in their education. College education authenticates knowledge. Certification authorizes it.

4.10.13 Head-hunters were suggested as an option in terms of a source for qualified professionals who would know the subject area, from the premise of the head hunters knowing the industry. **[7ES]** However, in contrast, respondents identified that recruitment agencies are seeking individuals with "cyber" skills and if longstanding InfoSec professionals and IA practitioners do not explicitly reference "cyber" in their CV, they are discounted. **[15ES, 76S]** This lack of cohesion of purpose and messaging has not helped the collective industry.

4.10.14 In 2005, a strategic partnership between ISACA, ISSA (the Information Systems Security Association) and ASIS International (the American Society for Industrial Security) was announced in response to the convergence pressures on IT audit, information security, and physical security professionals. Unfortunately, there has not been much to show from the partnership to date, despite the potential for members sharing benefits and cross-skilling. It is difficult to find mention of the partnership on the websites of the three partners. However, the convergence pressures are still there, although audit independence obviously limits the extent to which IT auditors can sensibly merge with their colleagues in information, physical security, or other fields.

4.10.15 In 2017, the IISP embarked on the Chartered status process to create a Chartered Information Security Professional. However, the Worshipful Company of Security Professionals has already been awarding Chartered Security Professional status in conjunction with ASIS. The future implications are that those with existing certifications, qualifications and chartered status awarded from other

bodies, may have to duplicate the effort in order to maintain their perceived currency and credibility in the industry.

4.10.16 Table 9 below provides an overview of the available spread of resources for practitioners. Others have been identified in **Appendix II**.

Sector	Covered by
Government	USA (including NIST), UK (multiple outlets including CESG, CPNI, DWP, MOD, Home Office, Cabinet Office), Australia, Singapore, Germany
Industry	IBM, HP, Oracle, IBM, Tripwire, Microsoft, SANS Institute, CISCO
Professional Services Networks	Deloitte, PwC, Ernst & Young, KPMG
Professional membership bodies	IISP, BCS, IET, ISACA, (ISC)², ISSA, SABSA, BCS IRMA, ACS (Australian)
Not for profit industry membership bodies	IAAC, ISF, Cloud Security Alliance, SABSA, EC Council (International Council of Electronic Commerce Consultants)
Other bodies	ARMA, ACCA, BCI, IRMS

Table 9: Spread of Information Resources Available

4.10.17 NIST 800-100 was suggested as a good reference point, as was ISO 27001 on multiple occasions. The IAAC/IoD Directors Guides to Managing Information Risk were also mentioned as reference resources. These have been in circulation since 2004. **[20F]**

4.10.18 In 2016, this research inspired a series of workshops on the Profession led by IAAC. The output from this (IAAC, 2017) coined the term GRADE A to cover the breadth of possible actors across Governors; Risk Managers; Auditors/Assessors; Defenders (incorporating testers, analysis and operators); Engineers and Architects. The workshops and resultant paper corroborated these

findings – that there is an excess of industry duplication and confusion and that the profession does not present credibly as a result.

4.10.19 During PAR in **CS2**, respondents identified that there is a risk that due to the inward looking support of the silos, service providers are selling what they want to sell, not what the customer needs to buy. **[69S]**

4.10.20 The findings from respondents bore out that the risk of unprofessional, ill-informed decision makers was regularly witnessed. **[20F]** Delivering IA "... is only noticeable if it is absent (like the washing up and the bed making) and you get no medals for it!" (senior UK Government official, IAAC Symposium, 8 September 2010). Through the delivery of presentations addressing elements of this research, the hypotheses have continued to be tested and there is practitioner confirmation that there are those in the profession who already see that a) calling it cyber and b) not understanding the breadth of coverage are negatively impacting the ongoing skills crisis and reducing the success of the IA professionalism agenda.

4.11 Information Society

4.11.1 The research survey responses led to wider societal and industry related analysis and consideration, therefore the next two issues were not initially addressed in the Literature Review. See Memos at **Appendix I, Section 10.17, Table 26**.

4.11.2 The IoT is considered to be the next industrial revolution – the second digital revolution – and everyone needs to be prepared (UK Government Office for Science, 2014). One respondent identified that the InfoSoc will "bring about participatory forms of government, quite

different, in different countries". **[15ES]** The IoT is an ego centric "internet of me" place to inhabit. There is a "grand bargain" to be had between privacy and functionality. However, there is still insufficient awareness by the citizen with regard to their role, responsibilities and liabilities. GetSafeOnline has been around in the UK since 2006.

4.11.3 In the US there is a Cyber Security Awareness month (October) which has been adopted globally. There are other examples of efforts to raise awareness worldwide and yet citizens do not necessarily adopt the health warnings for their multiple connected devices: updating firewalls, anti-virus protection, avoiding clicking on unknown links and visiting non-secure sites.

4.11.4 Timberg (2015) provided a valuable write up of the challenges faced by building the connected future on an insecure foundation which is not fit for purpose. This signposted the 1998 appearance of a group of hackers from L0pht Industries before the US States Senate where they informed them that computers, were not safe — neither the software, the hardware, nor the networks that link them together. "The companies that build these things don't care, and they have no reason to care because failure costs them nothing. And the federal government has neither the skill nor the will to do anything about it" (Grand, 1998).

4.11.5 In the US, Congress has been actively involved in cybersecurity issues, holding hearings every year since the nineties. The UK NAO has provided similar reporting oversight. There is no shortage of data on this topic: government agencies, academic institutions, think tanks,

security consultants, membership bodies and trade associations have issued hundreds of reports, studies, analyses and statistics. The UK Government itself holds the statistical data to evidence that near 80% of the significant breaches experienced in the preceding three years were as a result of poorly patched systems where the vulnerability management was not kept up to date (Lucas, 2015, p.242). This does not positively position the security professionals responsible (nor their leadership).

4.11.6 The requirement to secure systems is based on perceptions of the value of the information those systems contain and the likelihood of any risk of exposure or loss. There are different views as to what constitutes important information and how such information can be treated within different organisational environments and cultures. The value of information and the need to adequately protect it have been important societal tenets for centuries. There is enough history available and this research has served to draw together many resources.

4.11.7 As an example of a situation made more complex by the InfoSoc, a known military installation had what was thought to be a good homepage on the Web. It showed an aerial view of the facility with buildings labelled “Operations Center” and “Technical Support Center”. It was valuable public relations, but it also provided valuable targeting information for those who might wish them ill. This situation was replicated in the private sector case study **[CS2]** where a Data Centre that served similarly sensitive clients had a video arranged for them by

Marketing, designed for advertising purposes. It unwittingly created the same risks, not something that the Physical Security people involved had initially considered until the InfoSec team engaged.

4.11.8 The InfoSoc has progressed apace, significantly enhanced as a result of the speed of technological developments and the reach of the internet to parts of the world previously unconnected. The speed of development(s) in many industries, in and of itself, leads to skills crises. Legislative, regulatory, industry standards and political changes can be shown to have had appreciable impact on the understanding of requirements for IP within the InfoSoc. Industry experts have been articulating the subject of IA, the reasons and need for it for several decades and yet progress to successful adoption still lacks corresponding speed in alignment with the pace of the InfoSoc - as evidenced by the increased volume of data lost or stolen and the number of systems breached. **[61S]**

4.11.9 The idiosyncrasies for each global sector have been creating fissures of broken understanding. However, in real terms, the concepts are the same; the risk appetites may be different, thus the implementation of controls must be adapted. Jacobson and Rursch (2013, p.12) captured the lack of mandate and the length of time for adoption of the IA frameworks in the following expression:

> .... Government, industry and higher education are to blame for letting security awareness campaigns serve in place of IT security literacy. Until we treat IT security as everyone's problem, and

employees and managers at all levels contribute to the company's security; we will continue to lose the security battle.

4.11.10 Each organisation owns its information, *not* the IT department. IT manages data, at a bits and bytes level. Information has been and can be used as a tool of war and indeed can be the theatre of war itself. Information war is economic war, not territorial and understanding of this is changing the dynamics of the protection mechanisms required (Denning, 2000).

4.11.11 IT vendors talk about Data Protection but, in reality, they do not mean this in the legal sense; they mean it in a technological sense. There are vendors claiming that encrypting data will address the requirements of the EU General Data Protection Regulation (EU GDPR). This presents a naïve understanding of the depth and breadth of IA required in order to deliver the full scope of IP, in the context of a regulatory landscape that is slowly adapting. The ongoing skills crises will continue to deepen as it is difficult to find people with the level of interdisciplinary specialisms required to address the IP implementation gaps, both philosophically and practically.

4.11.12 IA should be a central concern of business, government and citizens because: i) corporate value is derived from effective management of information risk; ii) society and government depends upon secure information infrastructures for the delivery of traditional critical services as well as for novel services; and iii) citizens need to take more responsibility for protecting the privacy and security of their information assets.

4.11.13 This will also be essential to the morale and confidence of the citizen in the InfoSoc, where information is the basis of all economic value. Though there are more questions than answers currently surrounding the future in the interconnected IoT InfoSoc, responsibility cannot be abrogated.

4.11.14 It may be that IA practitioners are suffering from too great a degree of scepticism which is having an impact on the capability to progress maturely. Sceptics tend not to believe in the requirement of basic foundations, of which there are many attributable to IA and, if properly implemented, would already be significantly reducing the current levels of risk to personal data, company reputation, trust in government and protection of systems and cyber space. Equally, there could be validity in the sceptic stance on the exact same grounds – the consistency of failures could be taken to imply that nothing should be done to address them (Meer, 2013 / 2015).

4.11.15 Information overload is often reported as being a deterrent to understanding and is recognised in science as being a concern as there can be "severe limitations on the amount of data able to be received, processed and remembered by the human mind" (Miles and Huberman, 2002, p.127). People also tend to ignore information that conflicts with an already held belief so they then get stuck in the change dynamic, not being able to move forward (appearing to be intellectually frozen). These inertia considerations will be taken into account during the analysis phase, ensuring consistency in judgement and evaluation is achieved.

4.11.16 Securely designed systems of systems are required from the outset. This will result in fewer system breaches; less loss of income, less impact to industry, individuals and society as a whole. Given that the Institute of Internal Auditors (IIA) has a set of International Standards for the Professional Practice of Internal Auditing, this is something that the IA industry should be working to emulate in order to raise their profile (IIA, 2009).

4.11.17 Alternatively, the security sector could cease to continue to try and force this change that has still not been effectively embedded after several decades and instead, given that security is *everyone's* responsibility. The "security market" could be restructured to ensure that the skills, experience, knowledge and ways of working necessary to embed the required IP techniques are available to every other industry.

4.11.18 Social media has shown exponential adoption (Fox, 2015). Accessibility to social media means people expect immediacy; they no longer have to wait for the evening news broadcast. The social norms of the internet are forming and storming on a daily basis. For as much as technology is changing the norms, it is also creating new problems and it will take people to resolve them. There have been other social anthropologists and scientists who have written about society and seen its adaptive changes over the era and decades.

4.11.19 Brin (1998, pp.295-6), in a seminal work on the Transparent Society, captured a number of options, following the thinking of others, concluding that the latest wave would be a *self-monitored society* -

auto-surveillance (self-scrutiny) becomes useful, necessary and then a compulsive part of daily life:

> Such a society is transparent and porous. Information leakage is rampant. Barriers and boundaries – distance, darkness, time, walls, windows and even skin, which have been fundamental to our conceptions of privacy, liberty and individuality – give way. Actions as well as feelings, thoughts, past and even futures are increasingly visible. The line between the public and the private is weakened; observations seem constant; more and more information goes on a permanent record, whether we will this or not, and even whether we know about it or not.

4.11.20 This was prescient and is emblematic of present day society. Brin also used the term "data smog", noting that it would lead to "pollution" (Ibid. p.300). This resonates with a shift in IT industry focus to "Big Data" and the need for the roles of Data Analyst and Data Scientist, particularly in the Security profession, in order to "mine" the data and provide "security intelligence" / "actionable intelligence" back to management and leadership. These terms are in their infancy in socialisation across organisations.

4.11.21 Thomson Reuters (2013a, p.4) suggested that "true behaviour change may best be achieved by more intelligent use of existing tools, such as work quality supervision and information flow, rather than by chasing an elusive "mind-set change". Schneier (2015a and 2015b, p.238) also addressed the theme of data pollution in 2015:

> Data is the pollution problem of the information age, and protecting privacy is the environmental challenge. Almost all computers produce personal information. It stays around, festering. How we deal with it -- how we contain it and how we dispose of it -- is central to the health of our information economy. Just as we look back today at the early decades of the industrial age and wonder how our ancestors could have ignored pollution in their rush to build an industrial world, our grandchildren will look back at us during these early decades of the information age and judge us on how we addressed the challenge of data collection and misuse.

4.11.22 In September 2015, the UK Knowledge Transfer Network (UK KTN 2015) released their draft work programme for 2016-2017 which included a call for submissions for suggestions for ways to increase security adoption, with a focus on the InfoSoc under the banner “KTN 2020”. The researcher contends that this will be another exercise in the creation of new ways to solve known problems for which existing solutions were available. KTN 2020 is not encouraging anything other than repeated patterns of bad behaviour. Companies will have the opportunity to request new government money to address an old problem that remains unsolved due to lack of application of existing knowledge and coordinated effort. There is a lack of evident industry accountability and corporate social responsibility.

4.11.23 The scale of the challenge was previously identified: “IA demands that trustworthy systems be developed from untrustworthy components

within power-generation systems, banking, transportation, emergency services, and telecommunications" (Hamre, 1998). Anderson's 2015 report for UK Government entitled *A Question of Trust* (Anderson, 2015) provides a detailed exposition of the challenge of the scale of technological reach – and the impacts of that on society.

4.11.24 Security industry dialogue is inward-facing; the membership groups talk to each other about subjects they already know about. This creates an insular and parochial effect which needs a revamp in order for it to be effective for the 21st century information age. Globalisation is prevalent, with large businesses having employees working worldwide. Maintaining country specific bodies does not seem appropriate in this InfoSoc context. **[CS2]**

4.11.25 The world continues to connect devices at an accelerating rate. The known safeguards have been established, but are not being adequately installed, implemented and maintained and this is risking the fragility of the InfoSoc that can be easily shattered, particularly as the criminal fraternity continue to easily find vulnerabilities in the infrastructure. This fragility was further evidenced in the European Court of Justice (ECJ) ruling on the legal basis for transfers of personal data to businesses under the US Safe Harbor agreement (UK ICO, 2015).

4.11.26 In the context of the globalised IoT environment, the UK cannot stand alone. No single country can, for example, issue anti-spam legislation, given that the perpetrators of cybercrime are worldwide and do not respect geographical nor legislative borders. The same is true for

challenges presented by operating in the cyber domain, already addressed in the Cyber Trust and Crime Prevention work undertaken in 2003 (UK HMG 2003a), though the risks and implications of the extent of the global connectivity may not have been appreciated. Further detail is provided in **Appendix I, Section 10.18**.

4.11.27 There is no IA if not all participants (including citizens) are aware of, and take up, their responsibility. **[16FS, 52S]** In the future, this will require cross discipline effort from psychology, sociology and behavioral scientists. The protection of collective information resources – which requires IA – will be a defining challenge of national security, worldwide in the years to come.

4.11.28 Whilst articulation of the real, persistent and growing threat has moved from the technical journal pages to the front pages of worldwide media newsprint (both on and offline), the people challenge being seen is that the greater threats may be from complacency, ignorance, obliviousness, politics and budgets (Curmudgeon, 2015, p.39). The IA message has to be disseminated using the tools of the Information Age. Once wide understanding is genuinely achieved, the InfoSoc will regulate through the planned legislative changes combined with the increased prosecutions for data breaches.

4.12 Barriers

4.12.1 Barriers have been constantly identified throughout this thesis; for many respondents, the greatest concern was inaction. **[14F, 24T, 54S, 81F]** See Memos at **Appendix I, Section 10.17, Table 27**. Given the plethora of available approaches, standards, regulation, legislation, industry bodies, multiple overlapping and competing government agencies – this inaction may, in fact, be caused by paralysis, with those involved not knowing which way to turn.

4.12.2 A consistent theme reflected during the research study was that emphasis on ICT technology has had a negative impact on IA by providing a false sense of security. Antivirus vendors, patching, firewalls, IDS/IPS, access control are all necessary but not sufficient to protect confidential information. Change upsets and disrupts. Vendors do not want business professionals to look at other products nor to challenge their cost models. Decision-makers who supported the purchase of existing systems may fear a change in direction could suggest the original decision-making was flawed. Some respondents reflected that business practices stifle the realisation of good security through the attainment of a loss of security standards. **[35F, 38E, 38FE]** Other research undertaken resonates with the survey responses (Meer, 2015).

4.12.3 However, the scale of the challenge was identified some time ago: "The progression of information science collectively and individually perhaps does not have sufficient will or motivation to advocate its own cause successfully against the much stronger commercially driven

pressures of the IT professions" (Best, 1996, p.53). There is no group taking this forward. Vendors are accused of self-interest. Oltsik identified this when he stated: "if bad behaviour (such as confusion marketing or outright mis-selling) is regarded as normal by sufficient numbers of people in the industry, it becomes the norm" (Oltsik, 2014).

4.12.4 The "customer" can sometimes be hard to identify as they may be internal more than external:

> Executive management, with all their formal training, really does not have a foundation in security, and often a limited exposure to risk. They do not understand, or find benefit in learning our literary currency. Therefore, we are forced to try and adapt our terminology, used by limited practitioners, into the language of our disengaged masters - business equivalents, and to a closer equivalent financial audiences. In the process, in our attempt to be understood, we contribute to the fractured representations that we intend. The net result is that the language ... is imprecise. We bastardized it to be understood. The audience rarely deserves or benefits from our effort. There are a plethora of other causes, including the lazy and the well-intended but ill-educated. **[15ES]** This was also reference by respondent **[82F]** – "*Don't dumb down everything - train people up to the right level – we need to reverse engineer management*" (21 February 2014).

4.12.5 In all industries, there is a balance to be struck, none more so than in the IS realm. Things should be made as complex as necessary but no more so. Professionals cannot always be looking for a simple answer if it does not exist. **[35F, 39FE]**

4.12.6 Since the global financial crisis of 2007 imposed unprecedented budgetary restrictions on both the public and private sectors, new security solutions must be more efficient and cost-effective than the ones currently available. This has created a constant need to "do more with less" which has constrained the resources available to respond appropriately to a changing threat landscape. **[46S, 50S, 59S]** This is particularly relevant if the organisation has not historically invested appropriately in security controls and thus is starting from a weak security posture. The level of investment needed to improve security is higher than what would otherwise be necessary.

4.12.7 Senior management is continually incentivised to focus on revenue protection in order to strive and thrive: through status, recognition, end of year appraisals, marketing and sales techniques collectively displaying intellectual dishonesty. These behaviours put a strain on the ability of the organisation to maintain a level of ethical resilience (Raval, 2016).

4.12.8 When value protection is at odds with value creation, the dynamic changes, resulting in an inability to adequately risk assess the threat vectors. Conventional compliance has consistently been shown to provide a tick-box mentality that does not provide for security to be embedded horizontally across an organisation as opposed to being

tackled as a vertical silo. **[7ES, 73S]** The risk dynamic continues to confuse with evidence of risk aversion more likely than active risk management; with rewarded risk being at odds with unrewarded risk. Various resources for guidance on addressing these challenges are available (ACCA, 2010a/b/c).

4.12.9 As another example of a further wave of change in 2015, the UK Prime Minister set out his vision for a smarter state which would require greater consolidation alongside devolution of power (Cameron, 2015). There are a plethora of examples scattered throughout multiple research endeavours [including **CS1**] and many government reports, identifying duplicative work being carried out. A small UK Local Council intending to issue bus passes required data from colleagues within their own organisation. Those colleagues, incentivised to ensure they covered their costs, wanted to charge the transportation related team £15,000 to get the data right, due to a lack of IG and management having been applied. The data could not be relied upon not to contain reference to either dead people or people who could have moved away who were still showing on the relevant register. Such housekeeping activities need to be embedded as part of the IG activities, but should already have been in place as part of the data protection, and therefore compliance, activities. As Cameron (2015) stated – "It's not just about resources: it's about results".

4.12.10 Inappropriate controls coupled with the knowledge base increasing in the general public around privacy and security, brought on by publicised issues such as credit card numbers being published and/or

other private information being leaked, have changed the awareness of the cyber domain. The findings and the Literature Review identified that governance is misunderstood. The findings corroborate that enforcement is lacking; that policing compliance is difficult. It is a misnomer to believe that the CISO is responsible and accountable for the actions of business leaders.

4.12.11 Collective executive liability exists, much of which cannot be written about due to commercial sensitivities and risk. However, Home Depot, Target and the US Office of Personnel Management (OPM) breaches resulted in both Class Action suits and resignations at director level, the Chief Executive Officer (CEO) in the case of Target. Respondents confirmed and concurred that there is evidence of plausible deniability being the leadership stance. **[46S, 50S, 59S]**

4.12.12 Directors must, at all times, act in the best interests of the company and owe duties of good faith and trust. If a director fails in this personal duty, then he/she may be liable to the company for any losses occasioned as a result of this failure. This reality was well understood by a worldwide audience with the Volkswagen “deceit device” scandal in September 2015 (Hotten, 2015; Raval, 2016) and the subsequent identification of false data creation by both Mitsubishi and Nissan (TopGear, 2016). Ignorance is no defence in the eyes of the law. The lack of accountability and evidence of culpable deniability in action are creating barriers to successful risk reduction. **[35F, 39FE]**

4.12.13 The public expects that executives should be held accountable for not taking appropriate actions to protect their information processed, stored and transmitted through digital means. A Data Breach Litigation Report provides a comprehensive analysis of class action lawsuits involving data security breaches filed in the United States District Courts (Cave, 2015). A number of lawsuits were generated as a result of the Home Depot breach in 2014 and the Target breach in 2013. Prosecution of directors in the future is expected, which may change the incentives and behaviour.

4.12.14 Equally, personal liability exists, if an individual fails to ensure that appropriate internal control procedures and security measures are in place to prevent theft or destruction of proprietary information by hackers. Personal liability is linked to individual responsibility, the maintenance of which relies on high personal ethics (Stahl, 2004).

4.12.15 The influence of corporate change initiatives and rebranding was identified as a barrier by respondents. By way of an example, in the large private sector case study a new initiative was identified in the Asia Pacific and Japan (APJ) region, labelled as “Service Exposures”. The CISO Office undertook an investigation to identify to what this referred in order to ensure that there was no duplication of effort as all attempts were being made to standardise global processes for evidence collection, risk management and compliance reporting.

4.12.16 It transpired that the “Service Exposure” process was a risk management process by any other name that the region called it *Service Exposure* to cut through any resistance from accounts

regarding existing risk processes – with no acknowledgement of the level of duplication this would cause. It was being aggressively rolled out across APJ by management hungry for the visibility of risk and risk management. They were using one SharePoint per account but with a consistent model for each and had requirements (but not resources) to develop dashboard reporting. This was at the same time as the global CISO Office team were already working on the Account Risk Repository in which relevant information and evidence could be stored and which would be visible to the region (APJ) management.

4.12.17 The net result of this entirely separate initiative, as a company, was that when in receipt of either an internal or external audit and asked for evidence of risk, the company would have a whole region missing because they would be talking about Service Exposures and a data trawl would not evidence like for like. Renaming something does not help when the rest of the worldwide industry has no need to change its nomenclature. Change can be seen as an enabler. However, it is often a barrier in and of itself, but also as many are resistant to change. Equally, if efforts have been tried to implement new improvement programmes before, then that resistance can be understandable if there is evidence of previous failures. More information sharing can lead to more risk, which can create a barrier to adopting such initiatives. **[18E, 76S]**

4.12.18 The ability to deduce is being lost as a result of gaps in knowledge and a lack of ability to apply deductive reasoning. A number of respondents expressed concerns regarding this. **[22F, 35F, 39FE]**

4.13 Conclusions

> *By three methods we may learn wisdom: first, by reflection, which is noblest; second, by imitation, which is easiest; and third, by experience, which is the bitterest.* Confucius, Chinese philosopher and reformer (551 BC - 479 BC)

4.13.1 This chapter has been presented as a narrative discourse analysis in order to tell the story of the research process and findings. Signposting of respondent interaction has been interwoven to reference corroboration with the identified themes from the Literature Review and the survey findings.

4.13.2 The summation of the phenomena that emerge from the data analysis of the findings and the PAR are articulated below,: i) IA practitioners do not understand the ontology of InfoSec nor that of IA; ii) the shift in dominant narrative from IA to *cybersecurity* creates a schism that could have unforeseen consequences, diluting and narrowing practitioner and policy-maker understanding; iii) self-taught practitioners devalue the long term success of professionalizing IA; iv) lack of IA understanding results in higher cost(s) in the short term due to over-reliance on suppliers and technology products selected to reduce risk; and v) IA practitioners do not understand the relationships between InfoSec, IA, and IG. These empirically identified gaps are exacerbating progress of the UK government IA professionalism agenda.

4.13.3 In answering the first question as to whether IA professional practice could be improved through enhanced IA understanding, the answer is in the affirmative. The second question was designed to identify the

BoK and its impact on IA practitioner. The Literature Review identified core definitions that exist for IA. Discourse and content analysis of survey responses, interview transcripts, PAR and the supporting research findings presented phenomena that evidenced that the majority of respondents did not understand the term IA; the terminology used by practitioners is inconsistent. [**48S**] For many, InfoSec only incorporated the C of the CIA triad; the I and the A only, therefore, being applicable to IA. **[46S,68S]**

4.13.4 The McCumber and Maconachy frameworks are known by few, yet there are many propagating false views industry-wide **[9E, 31ES, 63S]**, including to UK Government, which is exacerbating improvement and achievement of the UK Cybersecurity strategy goals. The lack of detailed IA understanding should be of grave concern to policy makers, business leaders and government officials alike, given the importance of the subject area and how vital the effective implementation of IA is to the achievement of the stated objectives of the UK Cyber Security Strategy.

4.13.5 Much of the IA understanding is subjective and perspective based. Many of the private sector respondents operate in *vertical* industry sectors within a global outsourcing business. **[CS2, 45S, 50S, 66S]** As a result, they have not been exposed to wider industry experience. IA practitioners require a fundamental understanding of a wide range of specialisations, including digital forensics, fraud examination, systems engineering, security risk management, privacy, and compliance. The ability to interpret risks, review contractual language

and ensure that, in the event of a breach, their employer has adequate protection built into the contractual language is at risk. Establishing this understanding and keeping it up to date requires resources, with coverage as diverse as the field itself. These are broad areas of study for one single team to master and remain current in their understanding.

4.13.6 A sub question of the research was "How can we professionalise an industry that is not understood?". The researcher contends that it is vital that there is acknowledgement of this reality in order to avoid continuing down an ill-formed route. The evidence showed that volumes of standards and membership bodies have created barriers as paralysis can result due to the level of confusion caused. This was expounded in the Professionalism section.

4.13.7 The technological developments that have led to the current state of the InfoSoc have progressed through storage medium including microfilm, tape, disc etc. Within the context of this research, IA sits as a *subset* within a family of IM activity, according to Kahn and Blair (Ibid. p.14): i) Records management; ii) document management; iii) knowledge management; iv) enterprise content management; v) information security; vi) information privacy; vii) disaster recovery; viii) customer/client relationship management; ix) storage management; and x) data mining.

4.13.8 The UK Government approach has been largely department centric. As an example of duplicative wastage, the UK HMRC ran a different professionalism framework for contractors than that available from

either the Cabinet Office or CESG. Role based assessments versus skill based assessments need to be reviewed (IISP board meeting, 20 October 2015).

4.13.9 By 2020, the intention is to have cybersecurity as part of the UK national curriculum, although by then the requirements may have changed significantly with the impact of the IoT, with generations who have only ever known an existence entirely and fully absorbed in the digital realm, in cyber space.

4.13.10 The ontology of IG needs to be clearly understood by IA practitioners as IG was identified by respondents as the wider field within which IA needs to be placed **[58S, 60S, 68S, 71S, 77S, 81F]** – thus signifying the progression from IA, to IG, answering the third research question: Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec through to IA. This key finding was fundamental to the grounded theory development described next in Chapter 5.

Part 3 - Framework Refinement, Experiment and Discussion

In this part, the Grounded Theory is developed and refined as the research questions have been critically examined and the theory developed throughout the research period.

*The case studies [**CS1** and **CS2**], available in Appendix II, have contributed to the Grounded Theory development.*

This part closes with the research conclusions, shows the research contribution to knowledge and states areas for future research.

5 DEVELOPING A GROUNDED THEORY

5.1 Introduction

> *The idea of the computer and its infrastructure as primary objects of protection was always an aberration. It began that way because they were so expensive, large and difficult to replace. Today we throw them away. We are returning our attention to where protection, trust, and control should always have been – the processes and information that make up the landscape we manage.* Harry B. DeMaio (B2B and Beyond)

5.1.1 In order to synthesise the research findings, this Chapter describes the development of a Grounded Theory and the resultant holistic IG framework that comprises process, characteristics and best practices, answering the third research question: Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec through to IA?

5.1.2 Theories of professionalisation are brought together with a discussion of different types of professional identity and professional knowledge in order to show how the lens of professionalisation helps to make sense of the findings in Chapter 4.

5.2 Why Ontology Review?

5.2.1 Ontology - a lexicon of terminology and meaning - reflects the structure of the world and constrains the problem definition. The purpose of ontology is to ensure that duplication of effort is reduced to a minimum. Taxonomy and lexicon work have been well rounded in the InfoSec industry. The work of Uschold and King (1995), Tsoumas and Gritzalis (2006), Abdullah, Sadiq and Indulska (2011), Raskin *et al.* (2001), Cherdantseva (2014) and Arara, Fgee and Bargelail (2015)

have reviewed components of IA Ontology. Willetts (2008) created an IA Architecture (IA^2) and provided an in depth end to end IA enterprise life cycle management (ELCM) approach.

5.2.2 The goal of an IA Ontology is to provide a common vocabulary, reduce ambiguity, express needs, and facilitate action. IA currently lacks a distinct professional identity as a result of having neither, given that all are "borrowed" from InfoSec and there is currently too much terminology blend. Figure 35 shows the breadth of scope expected to be covered by various IA frameworks:

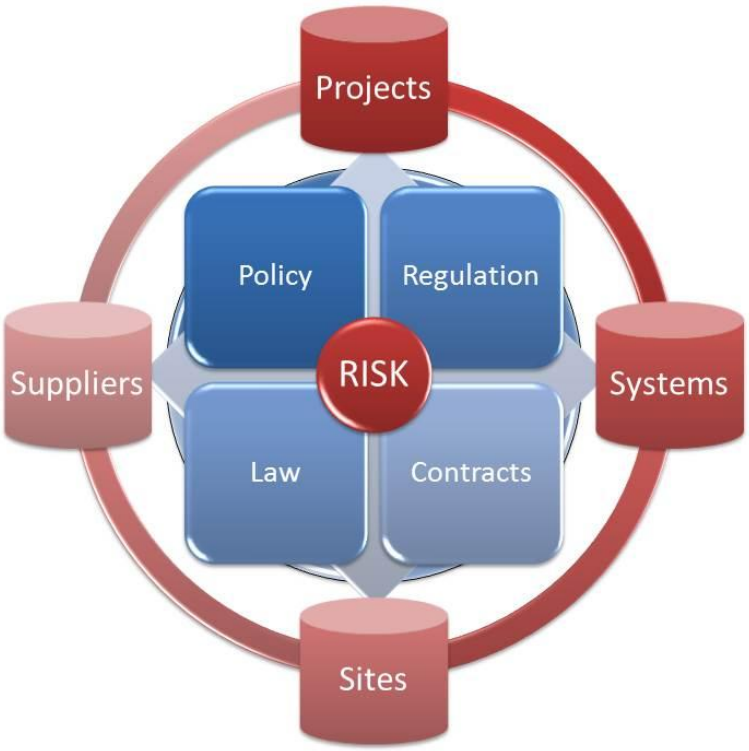


Figure 35: Mature IA, Source: Clarke (2015) and Tsoumas (2006)

5.2.3 The scope of involvement required for IA is depicted in Figure 36:

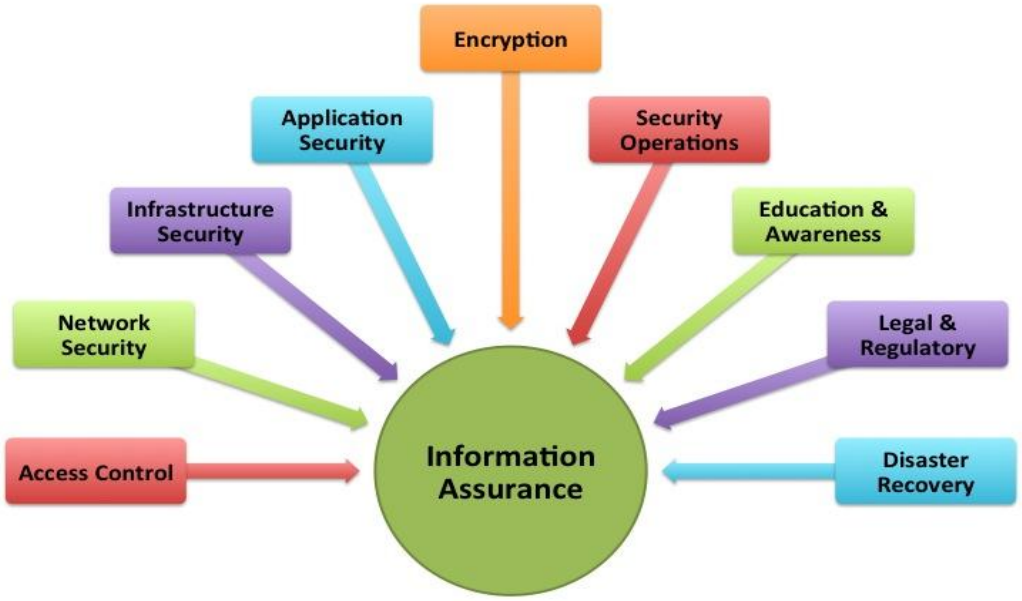


Figure 36: IA is a Shared Responsibility, Source: UNC Charlotte (2015)

5.3 GRC Revisited

5.3.1 As identified in the Literature Review, GRC is an acronym widely used in the Americas by large, multi-national corporate private sector businesses. OCEG (2007) recognized that GRC had historically grown up from separate, largely fragmented organisational initiatives. In order to address this shortfall, the objective of the OCEG was to develop an integrated, standardized approach to implement a coordinated GRC programme with specific accountability and oversight seeded through to a designated individual of suitable organisational seniority – or a committee at a strategic level – and to ensure board level fiduciary oversight with accountable stakeholders.

5.3.2 GRC is structured in that order for a reason, as an organisation needs to start with **G**overnance (of its PPT), identify its **R**isks and manage

(reduce) them, then evidence **C**ompliance. OCEG (2009a) identified the benefits of operating this system of PPT: i) enables an organisation to understand and prioritise stakeholder expectations; ii) sets business objectives that are congruent with its values and risks; iii) achieves objectives while optimizing its risk profile, and protecting value;; iv) operates within legal, contractual, internal, social, and ethical boundaries;; v) provides relevant, reliable, and timely information to appropriate stakeholders; and vi) enables the measurement of the performance and effectiveness of the system.

5.3.3 GRC is *not* about a single individual owning all the elements. GRC is expected to be a federation of professional roles working together in collaboration to achieve sustainability, consistency, efficiency, accountability and transparency (Howard and Prince, 2011, p.44) namely: governance; strategy and business performance management; risk management; compliance; internal control' corporate security; legal; IT; business ethics; sustainability and corporate social responsibility; quality management; human capital and culture; audit and assurance; and finance. GRC is also *not* about silos of risk and compliance operating independently of each other, nor is it another label for Enterprise Risk Management (ERM), although the R of GRC is intended to encompass ERM.

5.3.4 ERM is defined in Table 10 below by two leading organisations: the Risk Management Society (RIMS) and the Institute of Internal Auditors (IIA):

Body	Definition	Source
RIMS	Enterprise risk management is a strategic business discipline that supports the achievement of an organisation's objectives by addressing the full spectrum of its risks and managing the combined impact of those risks as an inter-related risk portfolio.	www.rims.org/resources/ERM/Pages/WhatisERM.aspx
The IIA	Enterprise risk management is a structured, consistent and continuous process across the whole organisation for identifying, assessing, deciding on responses to and reporting on opportunities and threats that affect the achievement of its objectives.	https://na.theiia.org/standards-guidance/recommended-guidance/Pages/Position-Papers.aspx

Table 10: Risk Management and Internal Audit: Forging a Collaborative Alliance, Source: RIMS and IIA (2012)

5.3.5 In particular, for the RIMS, the risk discussion is capital risk, financial risk – far beyond the technical and cyber risks the InfoSec sector discusses. Much of the risk discussion takes place at crossed purposes and greater skills are required to join these various disciplines together for the greater good of the organisations being served. Within the narrow sector of InfoSec, there is a continued lack of effectiveness at both understanding and capturing information risk.

5.3.6 Internal Audit provides an *opinion* on the veracity of the management *assurance*. To restate, Internal Audit does not provide the actual *assurance* – it provides an *opinion*. By providing an independent, second opinion, the Board is provided with a greater level of assurance as to risk management and performance. Governance provides Board level *reassurance.* These are subtle differences for which day-to-day operational management has had little cognizance of. Internal Audit looks at GRC as representing **G**overnance, **R**isk Management (RM) and Internal **C**ontrol (IC), (IIA, 2011). Figure 37 below represents the scope of Internal Audit review:

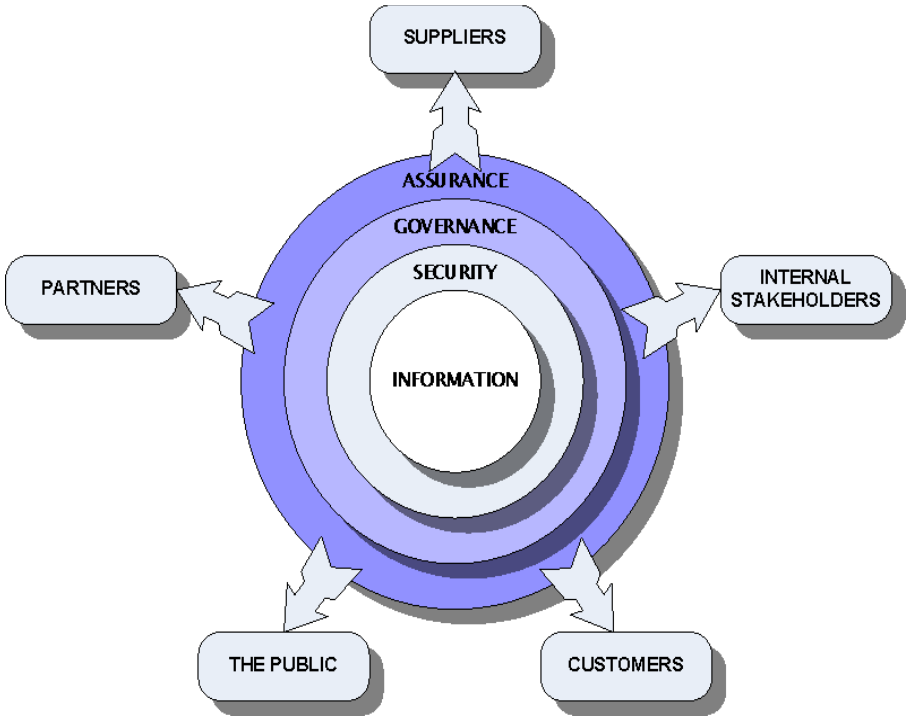


Figure 37: The Internal Audit review, Source: Taylor Baines (2013)

5.3.7 The COSO model provided the following pictorial representation of the scope of IA functions in Figure 38 below:

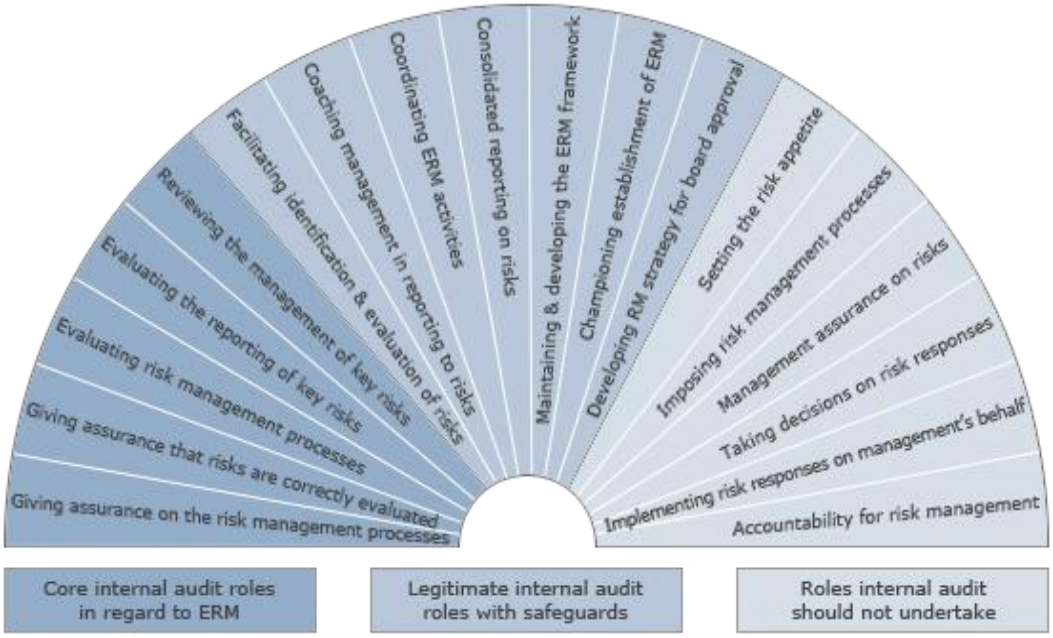


Figure 38: Internal Audit's Role in ERM, Source: IIA (2004, p.4)

5.3.8 Under the executive scope of Internal Audit, there are several disciplines that need to be conjoined in order to address the IoT, also referred to as the Internet of Everything (IoE). These have been depicted below in Figure 39.

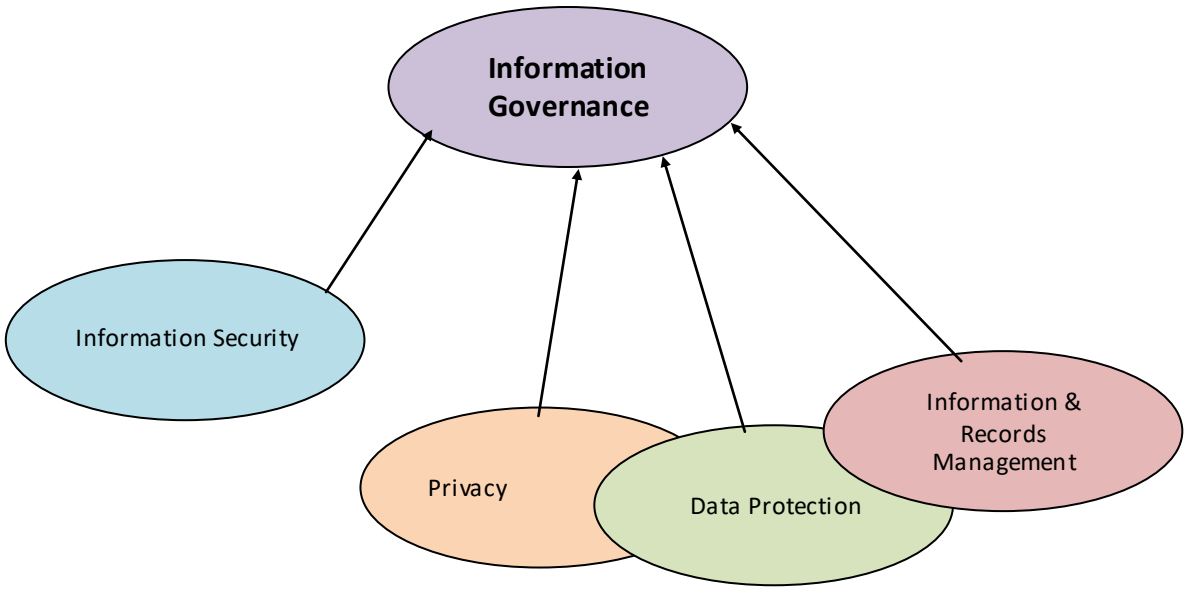


Figure 39: Disciplines to be Brought Together

5.3.9 Within the IT industry, GRC has been largely seen as a label for yet more technology or services consultants provide. The researcher contends that it needs to grow beyond the technology market rhetoric and focus. Technology plays a part, as evidence is required: i) to provide the assurance of achieving compliance to standards, regulation and legislation; ii) to show risk assessments having taken place and that controls are being implemented to effectively reduce identified risk; and iii) to show the breadth of governance an organisation has in place. KPMG (2010) encapsulated the breadth of GRC scope in the Holistic Model represented in Figure 40 below:

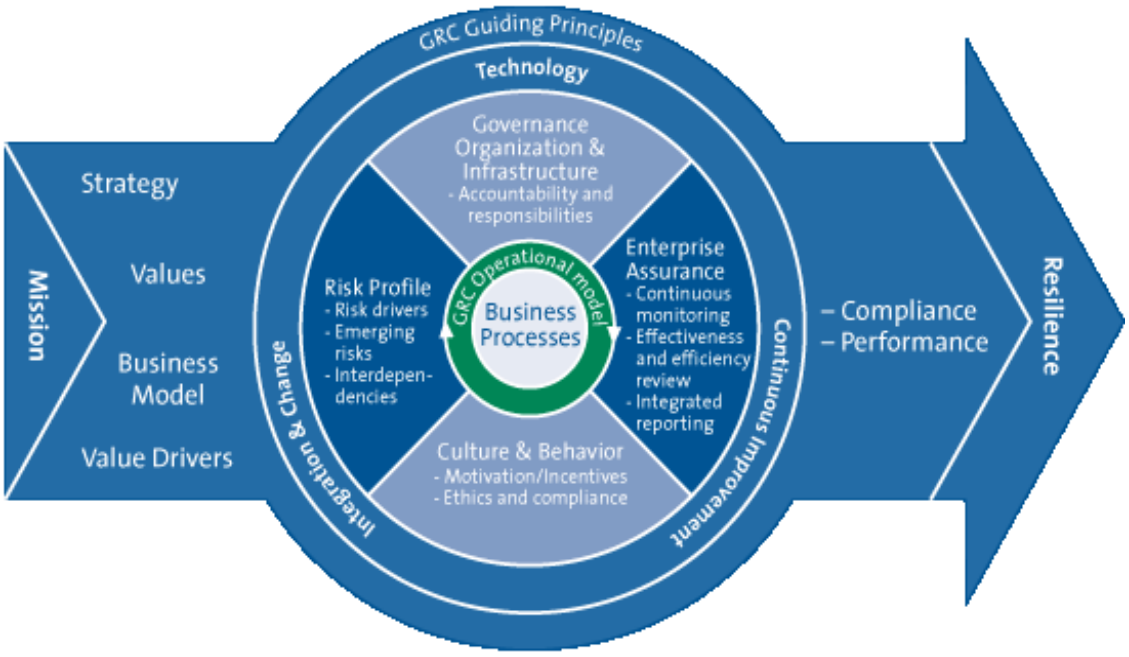


Figure 40: GRC Guiding Principles Holistic Model, Source: KPMG (2010)

5.3.10 The four components of Strategy, Values, Business Model and Value Drivers need to work effectively together in order to achieve compliance and evidence continuously improving performance. The ultimate goal for any organisation is resilience: the ability to deal with (or *flex against)* ongoing change, be it internally or externally driven, however seen or unforeseen the circumstances. This requires a well-formed governance structure and broad interpretation of assurance activities, for which IA is a constituent active part.

5.3.11 There is also the *Committee of Sponsoring Organizations of the Treadway Commission* (COSO) - - covering ERM, since 2004. There is clear evidence of the intentions to absorb the internal controls framework into the risk management framework to provide an integrated business operational management framework, as depicted in Figure 41 below.

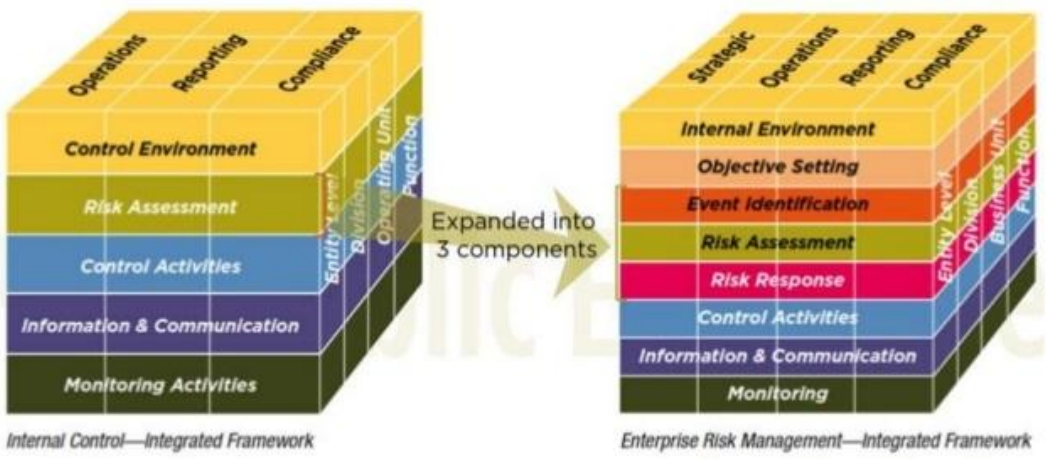


Figure 41: COSO IC to COSO ERM, Source: IIA (2010) and IMA (2014)

5.3.12 Depicted in Figure 42 is the COSO anticipated future goal state of ERM. The implementation gap between this anticipated future state and the present reality remains great, as a result of the ongoing separate operational teams present in most organisations.

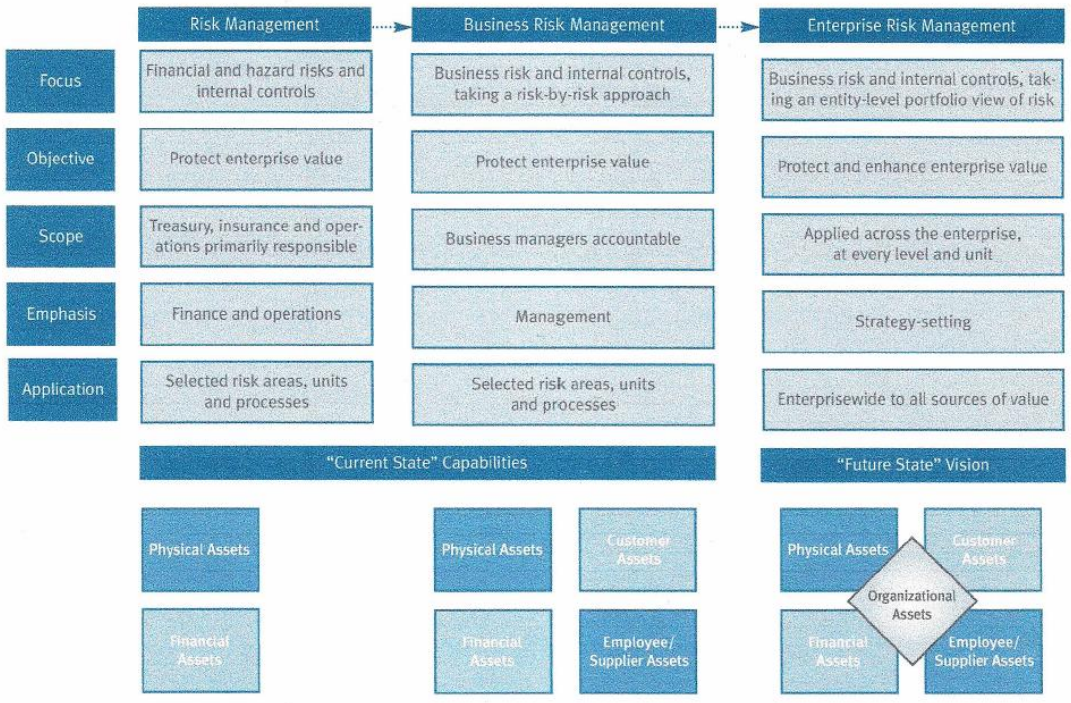


Figure 42: COSO ERM Model of Future Goal State, Source: COSO (2006, p.10)

5.3.13 Any initiative to implement a GRC programme in an organisation needs to be led by the executive; it needs senior level sponsorship in order to be effective. The same is true of any large change management programme. Once effectively implemented, the volume of available data can be significant, requiring aggregation and analysis in order to be appropriately mined and reported. This may imply new skills being necessary within existing teams. Historically, too many management reports are provided from raw spreadsheet data, none of which provides context or meaningful interpretation with regard to the actual level of risk being experienced and for which prioritisation of treatment is required, be it acceptance, transfer or reduction.

5.3.14 Business research shows that people like their jobs; their silos; and their spreadsheets; which leads to an insufficient outrage about what is not known (Mefford, 2014). However, in the corporate environment, 21st century management operates on the basis of the brevity of reporting (usually expressed on three slides, with only a few bullet points), often removing the sense and explanation of detail behind required decision making. This requires analysis skills in order to distil in-depth written reports.

5.3.15 Spreadsheets are simple to create, but complex to manipulate and manage. Many organisations are managing legacy systems and these are an important part of the infrastructure. The transition and transformation from their usage to the adoption of “as a service” vendor software offerings creates gaps where history has not been captured in terms of knowledge of the working of those systems. In

order to automate governance across the life cycle of information systems available, commitment in understanding of the impact of attrition of resources and intelligence occurring through both planned and natural wastage is required. This creates risks that must be fed into the GRC system to be managed ongoing.

5.3.16 In **CS2**, the researcher directly experienced both duplicative teams and redundant technology being accepted by a business going through continual transformation and people reduction. Management requires new skills to be more discernible with regard to the quality of the reporting it is receiving; requiring intelligence to be able to appropriately interpret the data for best results.

5.3.17 Any organisation must be able to evidence compliance with policy, with certifications; or mandated through legislation or regulation; and with best practice, if contractually obliged to do so. The results of compliance activities need to be included in strategy setting and formulation of initiatives, rather than always being in the position of providing reporting *ex post facto*.

5.3.18 The Board requires independent assurance that these activities are operating effectively, usually the purview of Internal Audit. However, compliance evidence is not the total aim. An organisation *must* be undertaking the activities for which the compliance evidence is the output. Achieving and delivering *security* – the act of ensuring the impenetrability of networks, of infrastructure and of information – is the ongoing endeavour. Risk activities should not be happening

independently of Compliance efforts; Governance needs to ensure that these are effectively drawn together.

5.3.19 Using a GRC framework approach helps to elevate InfoSec management through IA through to IG, with leadership level discussions due to the specifically targeted use of non-technical speech acts. The organisation needs to share information and have shared goals in order for it to be successful. The UK National Health Service (NHS) Information *Governance* toolkit had already elevated the dialogue by enveloping the activity under a governance umbrella.

5.3.20 All forms of risk and performance management need to be integrated, with budget, strategy and compliance. Functions, processes, and systems fragmentation needs to be reduced or removed in order to eliminate inhibiting performance. Quality, reliable, timely, current, useful and readily accessible information must exist and be able to be shared – and heard – in order for the organisation to effectively monitor and address the sensors available. Intelligent risk taking is as important as the management and reduction of them, within the context and boundaries of known compliance requirements with legislation, regulation, industry standards and societal expectations.

5.4 Ontology of IG

5.4.1 According to Gartner, IG is defined as:

> "the specification of decision rights and an accountability framework to encourage desirable behaviour in the valuation, creation, storage, use, archival and deletion of information. It

includes the processes, roles, standards and metrics that ensure the effective and efficient use of information in enabling an organisation to achieve its goals" (Gartner, 2010).

5.4.2 As identified by AIIM, "The term "IG" itself is charged with many meanings, largely dependent on the role of those hearing the term" (AIIM, 2014, p.2). Combining these available definitions, it can be interpreted that IG is intended to be a holistic approach to managing corporate information by implementing processes, roles, controls and metrics that treat information as a valuable business asset. Whilst IG is not wholly synonymous with corporate governance it can be considered more akin to "GRC for information". However, an IG specialist will not necessarily, by default, hold a depth of understanding of InfoSec. Nonetheless, taking this as a starting point makes it easier to progress from the currently insular and parochial, geographically bound IA approaches seen to date.

5.4.3 The IG Initiative (2014a) provided a different definition: "the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs". IG Initiative research (2014b, p.29) identified a Responsible, Accountable, Consulted and Informed (RACI) matrix for IG programme roles, as shown in Figure 43 below:

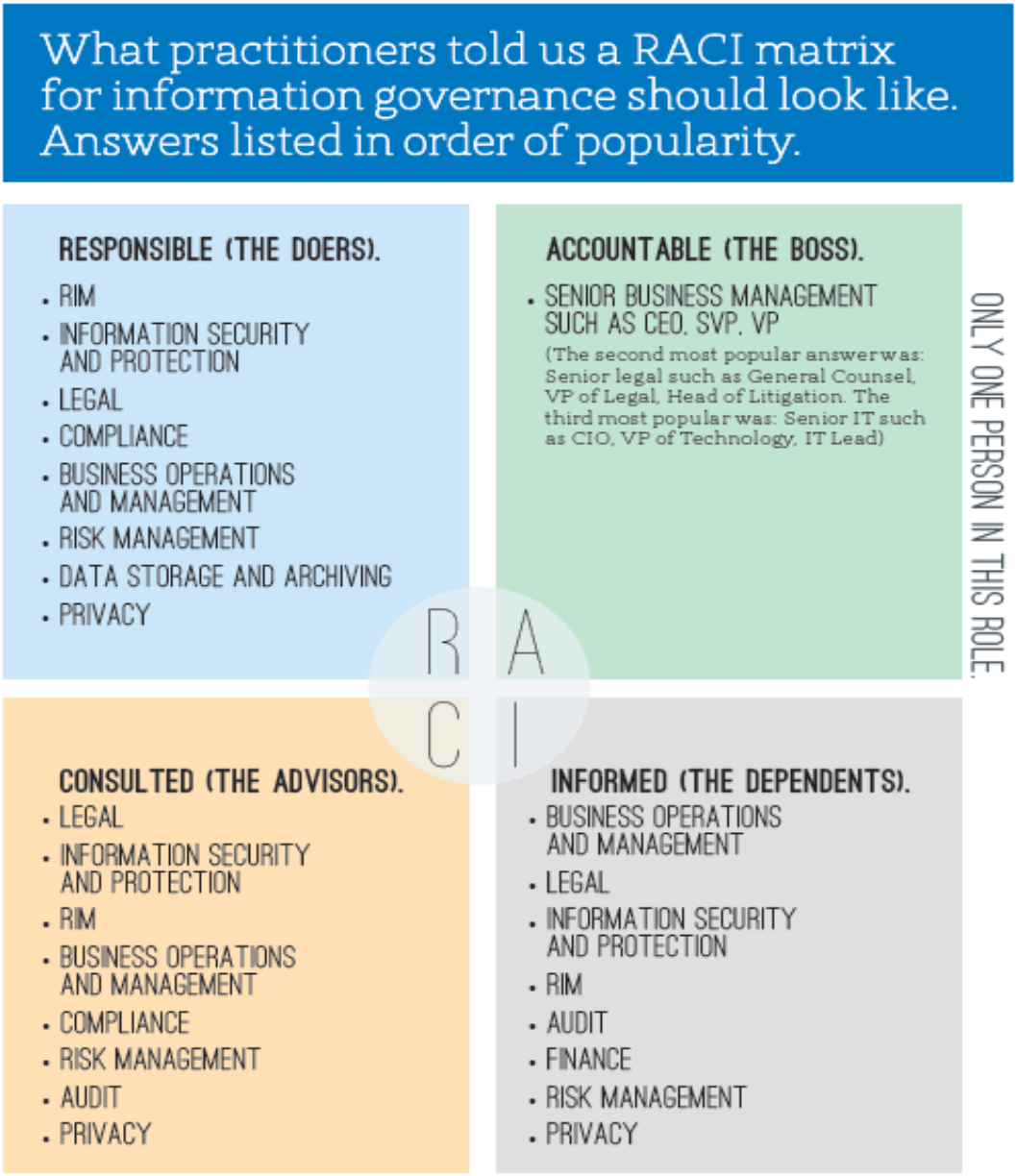


Figure 43: IG RACI Matrix, Source: IG Initiative (2014b, p.29)

5.4.4 The same IG Initiative research (2014b) identified the breadth of IG scope as outlined in the wheel in Figure 44 below:

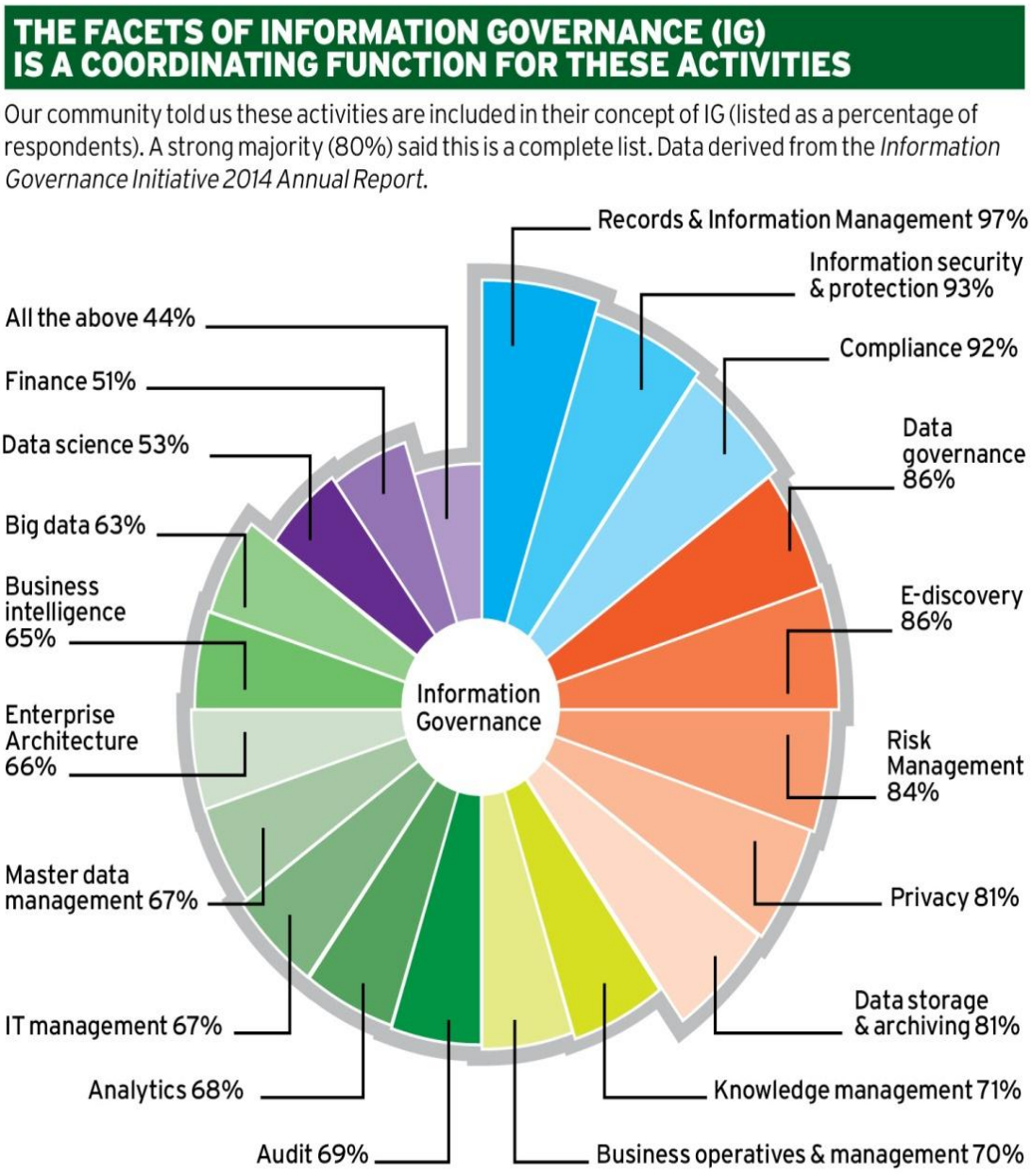


Figure 44: Facets of IG, Source: IG Initiative (2014c)

5.4.5 An IG Reference Model has been in existence, shown in Figure 45, since 2012. By the rhetoric used, the focus is Information and Records Management (another IRM) at its core but does not require much interpretation to extend it to incorporate IA.

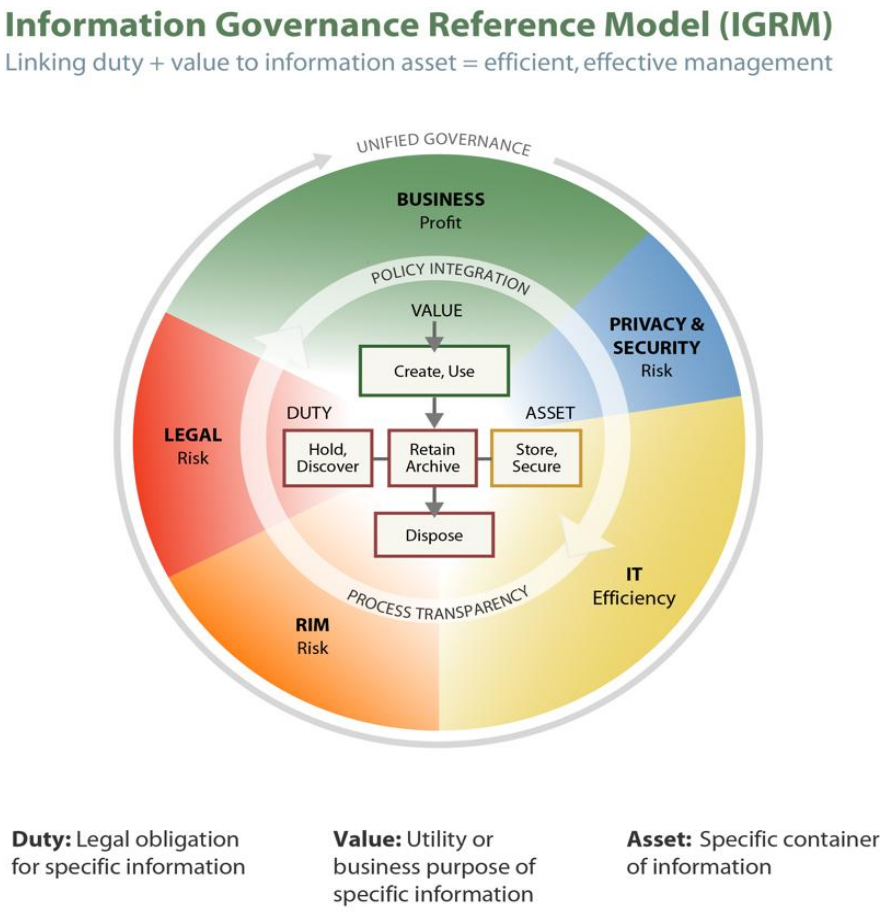


Figure 45: IG Reference Model © v3.0, Source: EDRM (2012)

5.4.6 Bringing together the activities of operations (doing), management (controlling) and the environment (information and the supporting technology) requires a level of sustainability that is challenging given the lack of time available for appropriate reflection when faced with continual organisational and societal momentum. This reality was borne out in the work of DeMarco and Lister (2013).

5.4.7 The representation of the maturity steps from InfoSec to IA to IG were previously presented in Figure 24 (page 98). This is where i3GRC™ enters, aiming to draw together the themes and models referenced in this chapter, from the top down, seeking to remove issues of interpretation, diffusion and confusion. The leadership and

commitment of management towards openness, honesty, integrity and ethical behaviour is important in change management and transformation programmes. Expectations with regard to employee behaviour when using digital devices has been discussed by many and the ongoing need to address this continues (McIlwraith, 2006).

5.4.8 IG has historically focussed on the governance of records. Most IG processes still reflect old approaches for managing physical records or documents, which in prior years formed the basis for managing a business. With the digital transformation of businesses and the ongoing increase in storage usage and as the price to procure media lowers, many organisations are left sorting the “wheat from the chaff”, reducing “electronic fluff” in favour of identifying the transcendent from the trivial. IG contains a strong element of striking a balance between risk, cost and value in the creation and storage of information. The elements of risk management are common in theme with IA, where risk mitigation is part of the activity wheel.

5.4.9 IG in the UK NHS (as per the aforementioned toolkit) includes: i) IG Management; ii) Confidentiality and Data Protection Assurance; iii) InfoSec Assurance; iv) Clinical IA; v) Secondary Use Assurance; and vi) Corporate IA. Again, note the combination of terminology above. There are a number of areas for assurance and a number of mechanisms to measure the success of the implementation. IG in the NHS was subject to a review that investigated “the structures, policies and practices of the Department of Health, the NHS and its suppliers to ensure the confidentiality and security of all records, and especially

patient records, and to enable the ethical use of them for the benefit of individual patients and the public good" (Cayton, 2006). This should have been happening across the whole of the public sector, rather than having the health sector operating independently, particularly given the continuing requirements for greater information sharing. As Pugh stated: "obligation and value must be determined by business people making systematic, informed decisions – the "governance" in "IG" (Pugh, 2011).

5.4.10 IG needs a champion in the C-suite, but it is not clear whether existing CIOs will transform into being CDOs or Chief Information Governance Officers (CIGOs), or whether new positions need to be created either as peers of the CIO or reporting to them. However, there is a risk that the boardroom cannot manage multiple Chiefs trying to be heard, which diminishes the effectiveness of the intended results.

5.5 Contextual Analysis

5.5.1 More complexity in the system hierarchy is leading to more human error and weaker system security, as well as a reduction in intellectual capital. These are intrinsic problems of the information age. As a triangulation of industry, research and theory is always required, at present, industry needs to catch up. However, due to the lack of reflection time, there is evidence of repeated patterns of erroneous behaviour. Coles-Kemp (2008) identified the blurred boundaries when reviewing InfoSec management system (ISMS) implementation against the Beers Viable System model.

5.5.2 Organisations have become so large and cumbersome with the volume of roles, disciplines and teams involved that it can take too long for tier 5 (usually CEO level) to hear what tier 1 (operational administration) have been telling tier 2 (management support) and by the time it reaches tier 3 (management) the information has been diluted beyond what tier 1 told them. The researcher suspects this will be found to be at the core of what happened in the case of Volkswagen in 2015. The reality should not be of surprise, given that others have written about it:

> One of the faults with current governance and management practice is that it is fuelled by the notion that the higher up you are in an organisation, the less you need to know about operational detail. And yet, when we look at some of the recent security failures of European organisations, the source of the errors has been at the coal-face in the operational detail. (Holt, 2013, p.37)

5.5.3 This view had also been identified in Jones (2010):

> ... senior management didn't want to hear bad news – but that attitude is changing over the past 10 years and they now want to know everything. The next level down don't want to pass the bad news up to management. If there's a culture where people are trained across all disciplines and they understand each other's issues and the way the company works – then they don't get stove piped.

5.5.4 Historical analysis identified that this aspect of management awareness – or lack thereof – was prevalent as far back as 1969 (SC Magazine, 2011, pp.26-30). Management were unaware of the risks undertaken in their name. This can be seen in organisations where (underneath the systems jargon) there is often a lack of a common agreement between departments even on what risk means to each party.

5.5.5 By way of direct example, in January 2015 two tier 5 executives in the private sector case study **[CS2]**, made the following proclamations to an internal employee meeting: "We do security like nobody else on the planet" and "There is unlimited resource available for security issues to be addressed". These two statements were in complete contrast to what (management) tiers 3 and 2 knew to be the reality – a lack of financial wherewithal to fund required improvements; continued attrition of key staff; notable penetration test findings; audit findings – both internal and external – all grave in nature and rendering the company out of compliance with contractual obligations, failing in its fiduciary responsibilities to adhere to specific legislative and regulatory constructs at the time. This was an example of the disjoint between the message tier 5 receives from tier 4 and the ability to repackage it from tier 3 to tier 4 (Hotten, 2015).

5.5.6 Most IT frameworks described as addressing governance are, in fact, addressing management. Whilst the COBIT framework from ISACA – formerly the IS Audit and Control Association – is intended to provide a common language for business executives to communicate with

each other – the subject area of focus is IT-related goals, objectives and results (ISACA, 2010b). The challenge this presents is an assumption that these are somehow different or separate from business goals, objectives and results. Iterative changes in versions of COBIT have sought to address the gaps in the prevailing dominant narrative, but if the starting point is IT and implementation is effectively bottom-up, then this will lack top-down direction and support. Shanes (2011, pp.46-52) reviewed the IAMM and supporting Assurance maturity framework. As a model, there is an implicit distinction between governance and management embedded within the task areas. However, the researcher would contend that the framework language presents another example of confusion, endemic in the industry, given that IRM is an intrinsic activity in the achievement of IA and should, by implication, not be being accounted for separately.

5.5.7 Figure 46 below shows it is possible to plot current status against denoted maturity levels.

Maturity Model Criteria	Assessment of Maturity Against Level					Justification of Assessment & Recommendation
	1	2	3	4	5	
Leadership and Governance	GREEN	GREEN/ AMBER	RED			
Training, Education and Awareness	AMBER	RED				
Information Risk Management	AMBER	RED/ AMBER	RED			
Through-Life IA Measures	GREEN	GREEN	RED			
Assured Information Sharing	GREEN	GREEN	RED			
Compliance	GREEN	AMBER	RED			

Figure 46: IAMM Self-Assessment Guide, Source: UK CESG (2013, p.9)

5.5.8 Maturity models usually use numeric scales. This model differs, using a "traffic light" model. The Red/Amber/Green status is defined within the framework as below:

- **RED** – There are crucial deficiencies against the performance required at this level. Major elements of the business IRM and IA processes have yet to be addressed.
- **RED/AMBER** – There are major deficiencies against the performance required at this level. Major elements of the business IRM and IA processes are not being addressed, and there are no credible plans to address the situation.
- **AMBER** – There are noticeable deficiencies against the performance required at this level. Some elements of the business IRM and IA processes are not being addressed, or whatever plans exist they have not been formally endorsed by the business.
- **GREEN / AMBER** – There are only minor deficiencies against the Business IRM and IA processes required at this level. Credible progress is being made against plans endorsed by the business.
- **GREEN** – There are negligible deficiencies against the performance required at this level. Business IRM and IA processes are fully met.

5.5.9 Archer RSA (2015), the globally renowned market leaders in GRC software, proposed a maturity model, depicted in Figure 47 below,

which acknowledged the challenges of separate domains and provided a trajectory for comparison:

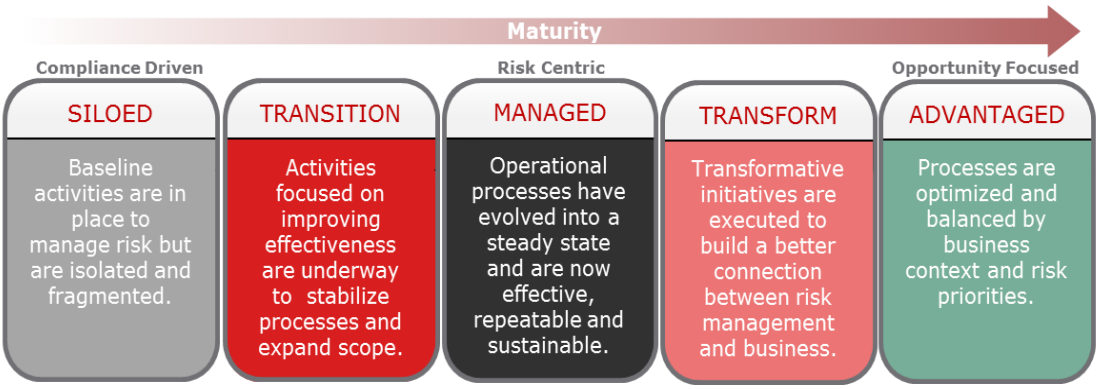


Figure 47: RSA Archer Maturity Model, Source: Schlarman (2015)

5.5.10 In implementation terms, basic security maturity has not yet been achieved by many organisations, rather it is compliance that has been achieved. The Compliance function is not always welcome at the boardroom table though the relabeled cybersecurity function is finding itself requested more often to provide leadership assurance as to the maturity of implementation of existing controls.

5.5.11 Management deals with compliance the same way a patient does on receiving bad news, creating delay and rationalisations (Deloitte University Press, 2015). Management sees security in a more vague fashion – it is too abstract. Day to day, a CISO could be measured on the basis of nothing going wrong, the organisation not experiencing a breach and not being in the newspapers / online media. For some types of management, this creates the response to reduce budget rather than acknowledge that the current levels of spend are working. Management, in whatever form, is used to being rewarded for creating value, profit, or whatever they are creating.

5.5.12 Compliance, security, and safety portend costs, and costs are to be avoided, minimized, and controlled. Other combinations of words currently in the industry include *data safety* within the Cybersecurity space and *safety critical systems*. The latter should be obvious given that industry is already seeing a need for greater alignment between security and safety constructs, particularly with the ongoing progression of driver-less cars and the Internet of Things (IoT).

5.5.13 The following formal definitions for security and safety provide a reminder of context: **Safety** is the state of being "safe"; the condition of being protected against the consequences of failure, damage, error, accidents, harm or any other event which could be considered non-desirable; and **Security** is the degree of resistance to, or protection from, harm. It applies to any vulnerable and valuable assets, such as a person, dwelling community, nation or organisation.

5.5.14 Associating security with safety can make for fleeting justifications. The challenge for those involved is to argue, and prove definitively, that the money spent to stop something from happening achieved that end. However, we have seen through the available regular and annualized breach reporting (Verizon, Ponemon, etc.) that we are facing talented adversaries. They have become necessary industry-led proof – with increasing regularity – that there are consequences for insufficient attention being paid to addressing risk reduction.

> *Large, global travel company does not have anyone on staff that understands how to do a Risk Assessment per NIST SP 800-30, Rev 1 or ISO 27005, as identified in the new PCI V3.0 standard. They run $500,000 in revenue every 60 seconds, on average, but they cannot run a standardized risk assessment.*
>
> *When you don't have the capacity to determine or quantify either safety, or security, you cannot claim that you are truly managing anything in particular. Where does that leave you? With Compliance, because there is a formula and process to measure that (even though clearly that is then subject to question as Compliance does **not** equal Security).*
>
> (Anecdote provided by respondent **35F**, email correspondence, February 2015

5.5.15 Lower security spend rates usually translate into issues with culture, lack of appropriate risk management, lack of governance and usually stem from an organisation that has failed to integrate security into business strategy and objectives. This reality arises when large organisations end up with multiple individual systems managed by dozens of autonomous development teams that are rewarded for speed and functionality, and who lack discipline about security. This gap between software development and security was most recently, publicly, made clear in the headlines with the security exposure in the Apple applications store (Guardian, 2015).

5.5.16 Further complexity exists in the number of external relationships being managed in order to deliver integrated services. A lower security spend rate can be argued as appropriate if there is evidence of a reduction in risk factors. However, without evidence of standardized security coding practices, secure code re-use (cutting down on security review costs, and even development costs); a forum in which to share best practices (because unfortunately employees are not paid to sit in collaborative meetings) then security reference architecture

methodologies are usually missing that would assist in achieving organisation “better - cheaper - faster”. Security architecture has the potential to deliver that trifecta, at the foundational level of any GRC framework. As Parker (2015) expressed it: “*Good security is when nothing very bad happens. And when nothing very bad happens, who needs security? Security seeks a “natural” lowest level. Periodic revitalization is necessary*”.

5.5.17 Technical assessments are seen as an overhead and are therefore removed to aid cost savings, resulting in systems builds lacking best or common practice and collaborative risk increasing. This is leading to normalizing the deviance (Dekker, 2011, p.198). The anecdote below helps to frame what continues to be the wicked problem at the core of this research.

5.5.18 Responding to breaches does not drive long term or cultural change, rather it drives reactive responses and too many security leaders take advantage of them to buy the latest technology or demand staff increases. Too many business leaders are happy to throw a little money at security because it looks like they are taking action and, in so doing, it gets the problem off their agenda. For context, most research timelines show that it takes thirty years to change a societal attitude - smoking, drink driving, obesity. Attitudes to security and privacy will continue to take time to percolate through to the fabric of society and for expectations to change, although the factors of the information age skew the timelines. It took thirty-eight years for radio

to thrive; fifteen years for television to become popular; and only four years for the internet to flourish.

5.5.19 Given the increasing interconnectivity and the global operations of many organisations, the researcher looked far beyond the immediate subject of IA. The World Economic Forum (WEF) Cyber Risk Framework, represented in Figure 48 below, captures much of the scale of thinking required.

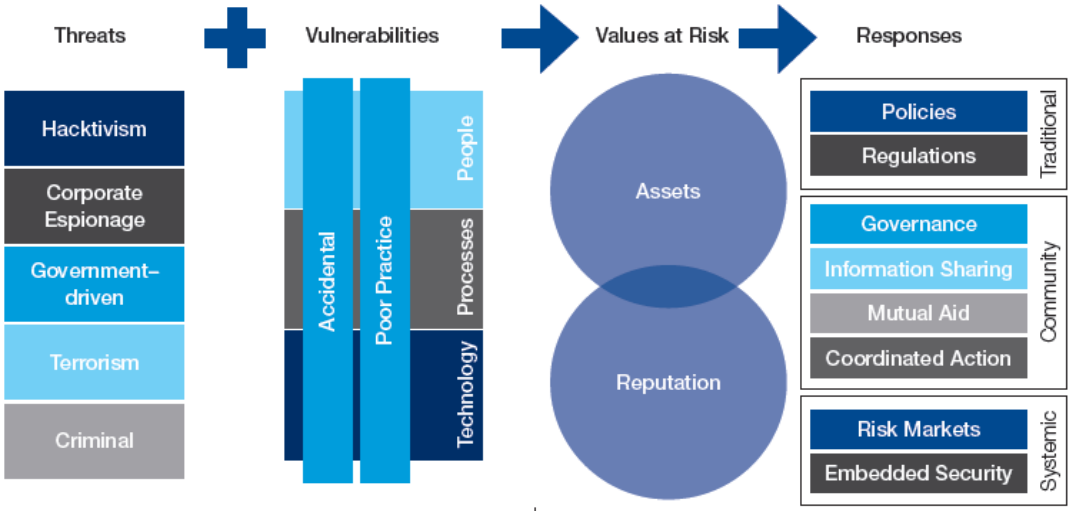


Figure 48: Cyber Risk Framework, Source: World Economic Forum (2012, p.13)

5.5.20 The CERT diagram, presented in Figure 49 below, shows the relationships that drive resilience activities at the Enterprise level – and is a Management Model.

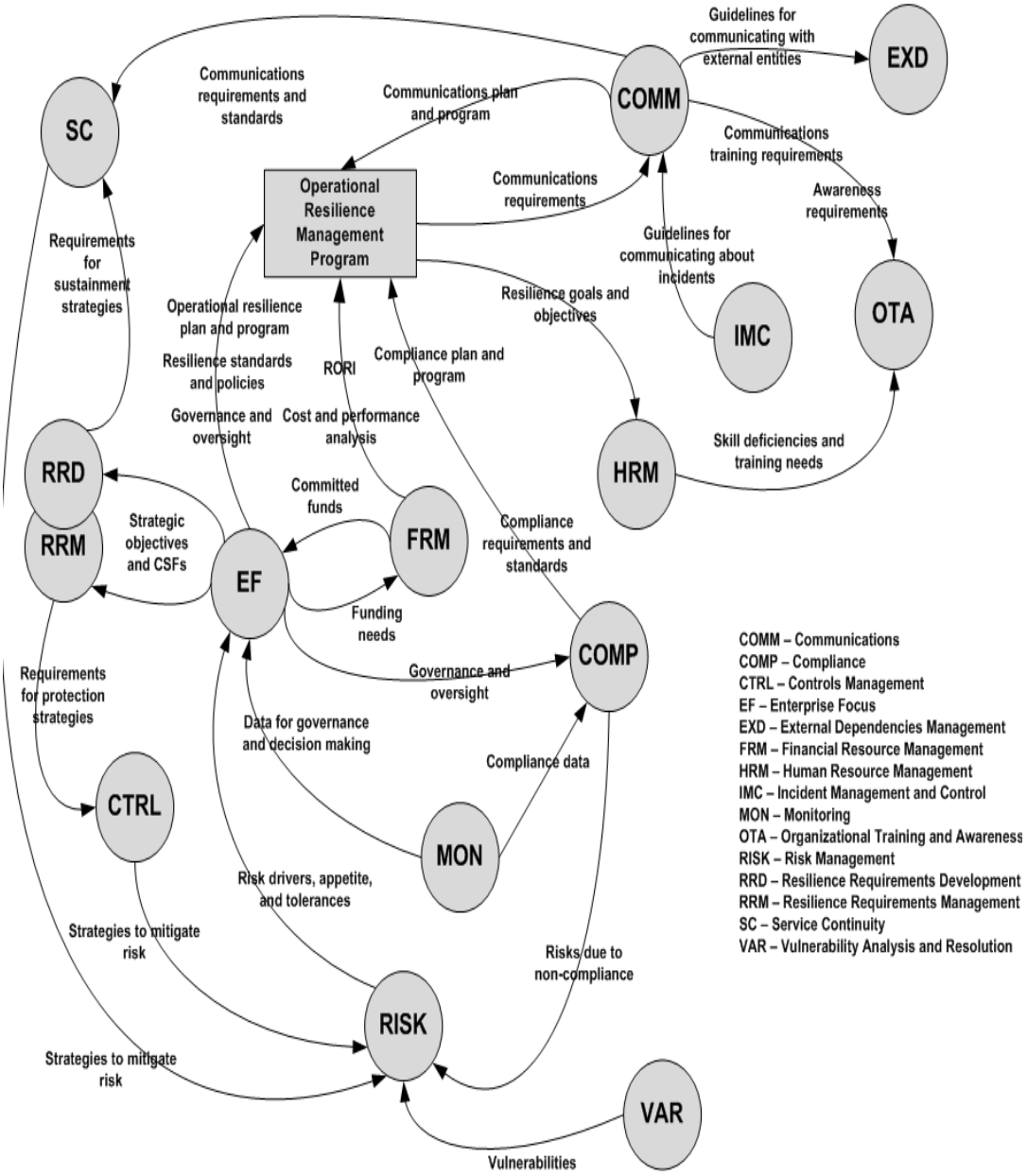


Figure 49: CERT® Resilience Management Model, Source: CERT (2010)

5.5.21 There is no explicit mention of IA or of IG, though what must flow throughout the model must be *information*, information that requires protecting end to end.

5.6 Theories of Professionalism

5.6.1 Professionalism indicates expertise in an area, reflecting extensive knowledge, mastery, skill or relevant qualification(s). Professionalism is accepted as being a consensus of norms, a collective commonality of approach to and execution of key roles, responsibilities, and activities that constitute the work undertaken by a profession. It is generally seen as the identification and expression of what is required and expected of members of a profession. Attributes of professionalism include: specialized knowledge; competency; honesty and integrity; respect; accountability; self-regulation; and image.

5.6.2 Brock (2006) provided a history of the past challenges of defining professionalism and identified relevant theories. Distinctions can be drawn between 'being a professional' which includes issues of status, reward, public recognition, and 'behaving professionally' which implies dedication, standards of behaviour and a strong service ethic (Helsby, 1996, p.138). Evetts (2003, p.558) suggested that being professional is not one, but a cluster of related concepts, in her examination of the changing nature of professionalism discourse.

5.6.3 Professionalism is demonstrated by competence; personal integrity; responsibility; accountability and public duty. One of the outstanding phrases heard during the Brexit vote in the UK in 2016 was when Michael Gove stated that "people in this country have had enough of experts" (Financial Times, 2016). This encapsulated a global experience labelled anti-intellectualism (Williams, 2014), following the rise of experts and indispensable roles, such as doctors, lawyers,

contractors, and stockbrokers. However, experts are human – and humans respond to incentives and so too many scandals were reducing faith (Koenig, 2012). Professionals have expertise, a prerequisite to socio-political influence, and (almost always) built-in networks of professional colleagues and clients (Spada, 2009).

5.6.4 In a UK parliamentary debate in 1992, Lord Benson defined nine obligations (principles) as to what constitutes a profession for the greater public good, represented in Table 11 below.

#	Obligation Description
1	The profession must be controlled by a governing body which in professional matters directs the behaviour of its members. For their part, the members have a responsibility to subordinate their selfish private interests in favour of support for the governing body.
2	the governing body must set adequate standards of education as a condition of entry and thereafter ensure that students obtain an acceptable standard of professional competence. Training and education do not stop at qualification. They must continue throughout the member's professional life.
3	The governing body must set the ethical rules and professional standards which are to be observed by the members. They should be higher than those established by the general law.
4	The rules and standards enforced by the governing body should be designed for the benefit of the public and not for the private advantage of the members.
5	The governing body must take disciplinary action including, if necessary, expulsion from membership, should the rules and standards it lays down not be observed or should a member be guilty of bad professional work.
6	Work is often reserved to a profession by statute - not because it was for the advantage of the members but because, for the protection of the public, it should be carried out only by persons with the requisite training, standards, and disciplines.
7	The governing body must satisfy itself that there is fair and open competition in the practice of the profession so that the public are not at risk of being exploited. It follows that members in practice must give information to the public about their experience, competence, capacity to do the work and the fees payable.
8	The members of the profession, whether in practice or in employment, must be independent in thought and outlook. They must be willing to speak their minds without fear or favour. They must not allow themselves to be put under the control or dominance of any person or organisation which could impair that independence.
9	In its specific field of learning, a profession must give leadership to the public it serves.

Table 11: Lord Benson's Professionalism Obligations

5.6.5 Professional bodies are structured to protect their reputations and the public interest simultaneously. They have a key role to play in the political consultation process. They also provide an important counterweight to centralised government administration through their systems of self-regulation (Spada, 2009). Shifts in professional regulatory structures took place within the broader context of a general political shift from interventionist to regulatory modes of governance within the European Union (op.cit.). In the UK, CESG responded to these changes by addressing nine attributes of Professionalism within the agenda for professionalising IA: i) Code of Ethics; ii) Competencies; iii) (Common) Body of Knowledge and Skills; iv) Knowledgebase; v) Register – record of all professionals vi) Practices and Principle; vii) Credibility; viii) Critical Mass and ix) Chartered status.

5.6.6 Other models exist, covering different attributes – for example, Brock (2006) identified seven dimensions of professionalism: i) *Knowledge* Specialist knowledge, unique expertise, experience; ii) *Education and training* Higher education, qualification, practical experience, obligation to engage in Continuous Professional Development (CPD); iii) *Skills* Competence and efficacy, task complexity, communication, judgment; iv) *Autonomy* Entry requirement, self-regulation and standards, voice in public policy, discretionary judgment; v) *Values* Ideology, altruism, dedication, service to clients; vi) *Ethics* Codes of conduct, moral integrity, confidentiality, trustworthiness, responsibility; and vii) *Reward* Influence, social status, power, vocation.

5.6.7 Bott (2005, p.16) was clear that the creation of a professional body was only the starting point. A level of regulation of members claiming relevance of professional skills was necessary to maintain trust.

> "The increasing rate at which new knowledge was becoming available and existing knowledge was being used in new ways led, in the 1970s, to increasing concern that professionals should keep their qualifications up to date and this process became known as continuing professional development (CPD). It can be defined as the systematic maintenance and improvement of professional knowledge and skills throughout an individual's professional working life."

5.6.8 Evans (2008) designed frameworks on the basis of the concepts of attitudinal and functional development. Attitudinal development is personal; functional development is organisational, attained by imposition. In discussing the "human factors" of IA, attitudinal *change* is often referred to as being required. This is different again to attitudinal development.

5.6.9 Combining these professionalism attributes, the expected structure of a profession has been mapped against the existing, overlapping, competing membership bodies in Table 12 below. Absent from the table are groups like APMG, ISF and IET. The former is an accreditation body, not a membership body; ISF is a corporate knowledge transfer body and the latter is an engineering body.

Aspect	ASIS	BCS	ISACA	(ISC)²	IISP	ISSA
Founded	1955	1957	1969	1988	2005	1984
Full-time occupation identified (critical mass of workers performing similar work / community of practitioners)	25,000	80,000 IT Professionals, of which 4508 belong to the Information Sec Specialist Group (ISSG)	140,000	125,000 - 23,000 in EMEA and over 5,000 in the UK	2600	13,000
Chapters, regionalised events	234 worldwide	Over 40 local branches and 50 specialist groups	Over 200 chapters worldwide	140 chapters; 34 in EMEA, 6 in the UK and Ireland	Local events in London, Manchester and Cheltenham	Over 135 chapters worldwide
Journals, magazines	Security Management	IT Now	ISACA Journal	InfoSecurity Professional magazine	Pulse magazine	ISSA Journal
Training or educational programmes provided	Yes	Yes	Yes	Yes	No	Yes
CBK/BOK	Yes	Yes, SFIA	Yes	Yes	Yes, Skills Framework	Yes
Entry requirements and validation process, competencies assessed		Yes	Yes	Yes	Yes	Yes
Code of ethics established (internal and external)	Yes, since 1957		Yes	Yes	Yes	Yes
Code of Conduct		Yes				
Communications network				Yes	LinkedIn	LinkedIn
Practices and Principles			CoBiT RiskIT BMIS			
Tradition, willingness to act for the common good, recognition of public responsibility	Yes	Yes	Yes	Yes	Yes	Yes
Register – record of all professionals	Member directory	CLAS Member directory	Member directory	Member directory	CLAS Member directory	Member directory
Support of law provided (professional lobbies for legislation, legal protection and legal recognition)						
Credibility	Yes	Yes	Yes	Yes	Yes	Yes
Chartered Status	Yes, Security Institute – CsyP	Yes, CITP			Intending to achieve this	

Table 12: Elements of Professionalism - Spread of Duplication (figures accurate at October 2017)

5.6.10 In the researcher's opinion, it would be beneficial for both practitioners and all employers, if ISACA and (ISC)2 moved beyond promoting their individual certifications towards jointly raising the profile and value of both IT audit and information security professions. An IA practitioner (or their employer) in the industry could (and often does) end up paying fees for all of these bodies.

5.6.11 Credibility is an important attribute expected of a profession, needing to be incorporated into the soft side of social science and which is distinct from the technical aspects of IA (Kelly, 2010). There is no evidence that the groups and their membership lack credibility. However, this is a subjective quality. Whilst an individual can claim it of themselves, it can be difficult to quantify whether others recognize it of the profession itself, in spite of their individual professional identities. However, the researcher has witnessed a consistent lack of credibility on a daily basis but because it is contained within the profession and within organisations, it is not visible to a wider audience and is therefore not acknowledged.

5.6.12 There are several types of professional knowledge (Watzlawick, 1978, p.26): i) **Propositional** – knowledge of content concerns the underlying theoretical basis of practice; ii) **Process** – the processes in which professionals engage whilst practising; iii) **Personal** – knowledge about self; and iv) **Value-based** – moral and ethical values and the beliefs one holds. The gap identified by this research is *propositional knowledge.*

5.6.13 Bott (2005, p.18) discussed the concept of "reservation of title", for professionals in areas considered to be in the public interest. Under the Architects Act 1997, it is a criminal offence to call yourself an architect unless you are registered with the Architects Registration Board. This sanction aspect is tied to "reservation of function", a restriction by law, to people with appropriate qualifications or to members of particular specified professional bodies. For example, only members of the Institute of Chartered Accountants in England and Wales or Association of Certified Accountants are allowed to audit the accounts of public companies. Nonetheless, anyone can call themselves an accountant, so both reservations are not always tied together. The mechanisms required to address this professional regulation do not exist in an IA context.

5.6.14 Veterinary surgery is an example of both. Under the Veterinary Surgeons Act 1966, you are not allowed to call yourself a veterinary surgeon unless you are registered with the Royal College of Veterinary Surgeons (RCVS). In order to be registered, you must have proper qualifications. In the US, title and function are controlled by means of registers maintained by State government. There is a blend of approaches and sanctions in UK professions.

5.6.15 Endicoytt-Popuvsky (2003, p.66) discussed sanction challenges from the US perspective:

> So far no IA educator has been held legally liable in court. ... Having an ethics course in an IA curriculum is good legal insurance against any liability claims. If societal concerns

don't motivate educators we should be motivated by the need to be legally protected in case problems arise from students misusing what we teach them.

5.6.16 Other industry sectors ensure that malpractice is punished. Nurses can be prosecuted for claiming to be a nurse and giving nursing advice or care if they are not on the Nursing and Midwifery Council (NMC) register. The NMC act as arbiters of the Conduct and Capability hearings for misbehaving nurses and ensure pin removal and the removal of the right to practice nursing in the future.

5.6.17 Research has shown that businesses are consistently asking that their needs be met in a timely manner even though they typically provide imprecise statements of their needs (Miller, 2013). In response, the IT community has developed the concept of the "requirements specification" that sets out the precision needed by the enterprise architect, software engineers, and others. An agreed-upon requirements specification is therefore frequently the starting point for many IT transformation programmes, and service-level agreements that encapsulate how the finished solution is to be delivered operationally. These documents are mostly created by an IT service provider who might also deliver the product and judge the outcome. However, incomplete or incorrect requirements specifications are commonplace (Miller, 2015).

5.6.18 This assumes the existence of either project or programme management teams. However, security teams lack these resources because the area is often underfunded, under resourced and

unsupported, despite running large, transformational projects which should have had an analysis of business requirements undertaken in order to ensure the expected benefits that should be realised.

5.6.19 The competency of understanding of contractual language and contract management needs to be added to the new competency framework developed by the work of Valentine (2015). Given the maxim “the contract is king”, an IA practitioner needs to be able to review supplier/contractor/customer relationships and to engage with Procurement personnel. From the outset, a contract must be constructed on the basis of what is required within the bounds of the legislative, regulatory and industry standards relevant to the organisation and their sphere of geographic operations.

5.6.20 Commercial pressures continue to override the ability to embed IA into system design. It continues to be expensive to implement technical security measures to protect information assets adequately. If these are not in place, then systems are vulnerable and weaknesses are prone to exploitation by unknown threat actors. A lack of security may be evident in the event of a breach. There is often a visible financial impact, be it stock price, share price or profit margin. Post breach reparation is required, including managing brand damage. Organisations must remove any conflict between job performance and security constraints by making security a part of workers’ job performance, in order to best achieve IA.

5.7 IA Professionalisation

5.7.1 The term "IA Professionalism" was embedded within the NIAS and is also reflected in the National School of Government programme Risk Management and Accreditation Specialist Programme, IA Professionalism Stage 3 for accreditors. [**Note**: – neither document was available online in 2015. The NIAS was superseded by the National Cyber Security Strategy.] An extract from the NIAS expected work programme is represented in Figure 50 below:

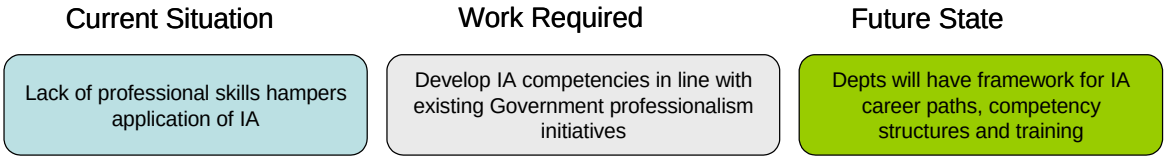


Figure 50: Delivering the IA Strategy, CSIA, Source: UK Cabinet Office (2007c)

5.7.2 The description in the supporting Action Plan below addressed a number of the themes identified so far, including that of the need for finance level understanding:

> Practitioners of IRM and the associated IA-related roles should be skilled to a level commensurate with their counterparts dealing with financial and other high impact risks. Clear competencies and career paths for IA-related roles across the Public Sector will be defined and linked where possible to existing qualifications and schemes, including ITPC, the Government IT Profession and the IISP (UK Cabinet Office, 2007c).

5.7.3 The visualisation of the UK IA landscape represented as a continuous feedback loop, shown in Figure 51, includes the first reference to professionalisation as part of the requirements for progression.

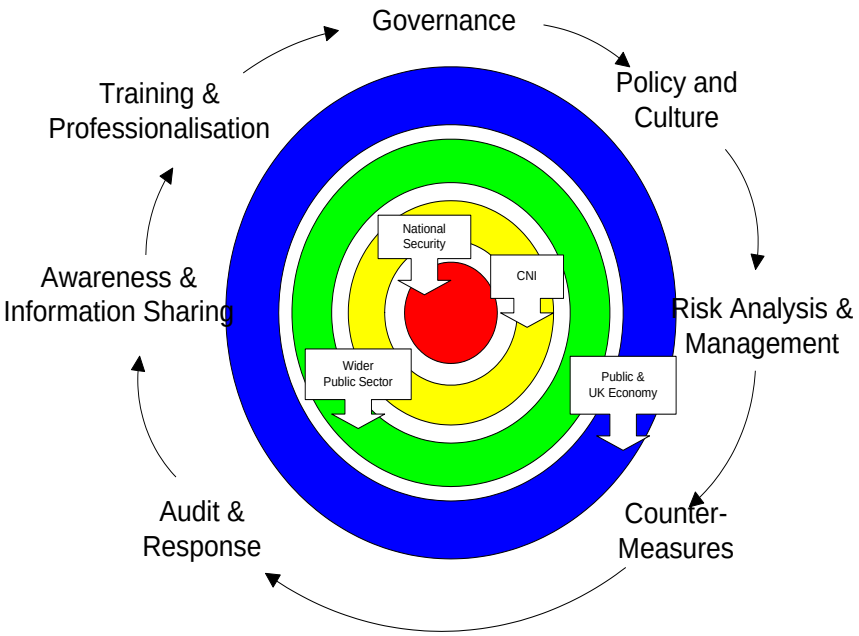


Figure 51: The UK IA Landscape, Source: UK CESG (2010h)

5.7.4 Research identified the required skills to fill the perceived gaps (Virgo, 2014), including the provision of greater education and training across a wider audience, as depicted in Figure 52 below.

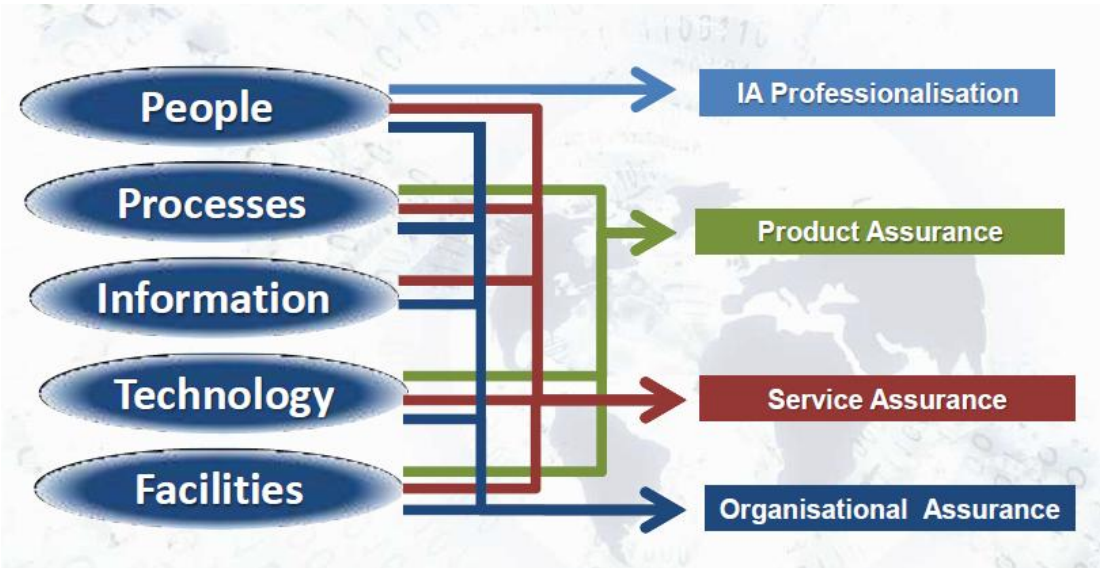


Figure 52: Pathway to IA Professionalisation, Source: Ensor (2011)

5.7.5 Coleman (2005a) identified a CBK, a skills framework for IA and the result ultimately was the formation of the Institute of Information Security Professionals (IISP) in 2005. The IISP was formed in 2005, with UK Government support. The researcher was a director of the IISP from 2011 to 2017 and is a member of the Accreditation Panel. There is evidence regularly appearing in IISP submission forms showing a lack of understanding as to the contextual meaning of Governance. However, equally, there is evidence of improvements in overall IA understanding.

5.7.6 Ensor (2011) followed this up by defining a profession as an occupation requiring extensive education or specialized training. A profession has cultural norms and cultural traditions etc. IA also has these but it is not clear that they are laudable. IA requires the right people with the right skills to protect and manage information. As with any sector, unprofessional decision makers are a risk. However, there are those who are motivated by a perceived morality in the profession, battling right and wrong, using technical skills to protect valuable business assets (ISACA, 2010b). Unprofessional decision makers are a risk. By implication, the right people with the right skills to protect and manage information will be adequately and appropriately trained.

5.7.7 In 2010, the ISF, (ISC)² and ISACA joined forces to create "The 12 principles of InfoSec" (Condon, 2010). However, these are no longer available online. Notwithstanding, in the researcher's opinion consolidation between the identified groups is long overdue. eSkills

(formed in 2003) worked with these groups to bring harmony across the various frameworks, particularly given the role of CESG in seeking to standardise and professionalise IA (in 2015, e-skills was taken over by The Tech Partnership). The task is exacerbated by the volume of participants in the space.

5.7.8 In the UK, an IA Skills Framework exists, as represented in Figure 53.

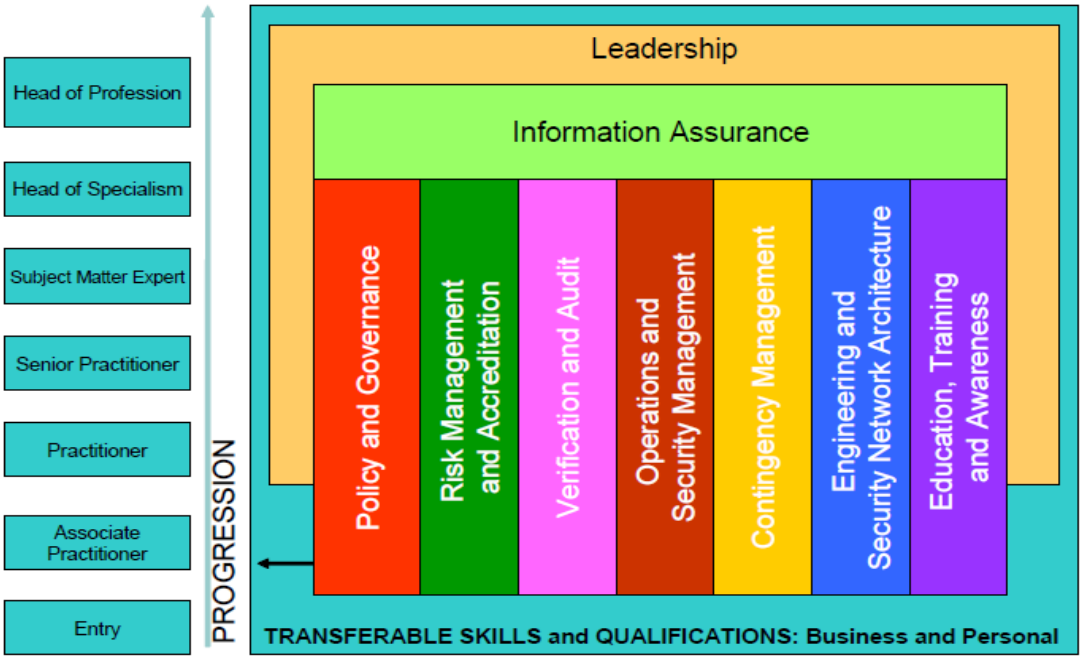


Figure 53: UK Government IA Framework, Source: Richardson (2012, p.211)

5.7.9 This framework is supported by the CESG Certified Professional accreditation scheme managed by three professional bodies on their behalf: the IISP with eSkills, the BCS and the APM Group Ltd (APMG). This is underpinned by the existing BoK contained within the BCS Skills for the Information Age (SFIA) framework and the IISP Skills Framework. However, a certification scheme does not ergo achieve professionalism and cannot be described as a professional route map for the IA industry.

5.7.10 As the UK CESG IA professionalisation agenda pitted three separate membership bodies against each other – APMG, BCS and IISP - this has diluted the potential impact of creating a single robust IA professionals membership body, and thus risked the realisation of an IA profession. They all represent some of the identified attributes of professional bodies, having: a community of practitioners; tradition; formal education/development process; a common body of knowledge (CBK); a communications network; entry requirements and validation process; recognition of public responsibility; willingness to act for the common good; code of conduct; and legal recognition.

5.7.11 Table 13 below shows skill areas assessed for Accreditation purposes:

A1	Governance	D1	Internal and Statutory Audit
A2	Policy and Standards	D2	Compliance Monitoring and Controls Testing
A3	Information Security Strategy	D3	Security Evaluation and Functionality Testing
A4	Innovation and Business Improvement	D4	Penetration Testing
A5	Behavioural Change	E1	Secure Operations Management
A6	Legal and Regulatory Environment and Compliance	E2	Secure Operations and Service Delivery
A7	Third Party Management	F1	Intrusion Detection and Analysis
B1	Threat Intelligence and Assessment and Threat Modelling	F2	Incident Management, Incident Investigation and Response
B2	Risk Assessment	H1	Business Continuity and Disaster Recovery Planning
B3	Information Risk Management	H2	Business Continuity and Disaster Recovery Management
C1	Enterprise Security Architecture	H3	Cyber Resilience
C2	Technical Security Architecture		
C3	Secure Development		

Table 13: IA Framework Skills Areas, Source: IISP, updated 2017

5.7.12 The first schools to teach security courses began doing so in the 1990s in the US, and they started offering degree programmes in 2000. The National Security Agency (NSA) partnered with other organisations to designate certain colleges and universities as Centres

of Academic Excellence in IA Education (CAE/IAE) and Research (CAE/IAE-R). This is the model that the UK CESG adopted. Figure 54 depicts the planned scope of work for CESG between 2010 and 2015.

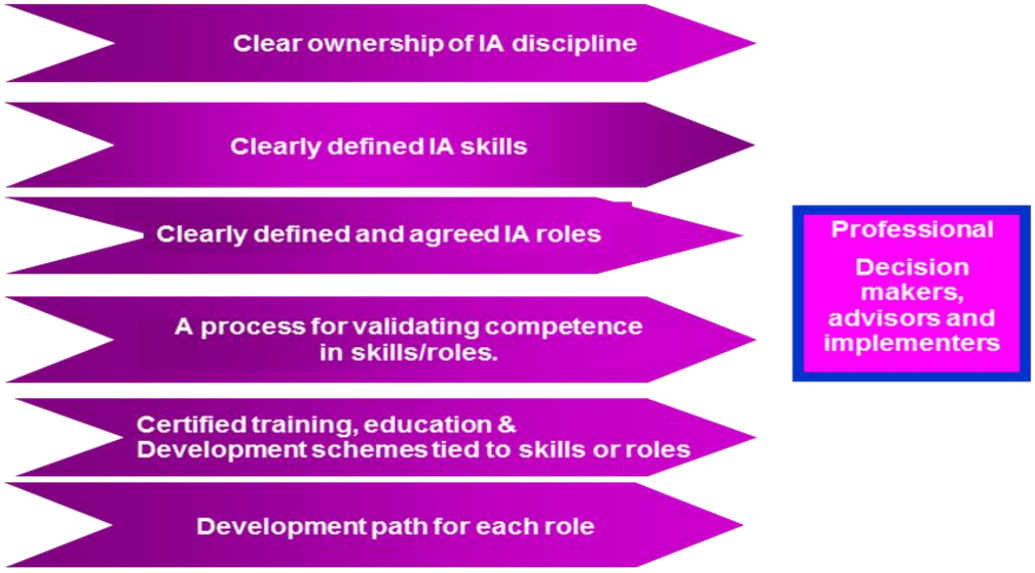


Figure 54: IA Professionalism Plans, Source: UK CESG (2010g)

5.7.13 The US Department of Homeland Security (US DHS, 2008) combined the available CBK and BOK into an Essential Body of Knowledge (EBK). There are multiple InfoSec related professional bodies, certifications and membership organisations. The Certifications are based on the aforementioned CBK, BoK or EBK. Depending on the certification undertaken by an InfoSec professional, they will be a member of a body by default. [See list in **Appendix I, Section 10.19**]

5.7.14 Conklin and McLeod reviewed the EBK, competency areas and the corollary roles relevant in the industry (Conklin and McLeod, 2009). In the UK, the BCS SFIA – the Skills for the Information Age framework and the IISP Skills Framework both co-exist. The IISP Skills Framework was updated in 2016.

5.7.15 The BCS Security Forum hosted an IS Professionalism event in November 2007 and another debate on IT and Professionalism three years later (BCS, 2010). In 2016, IAAC hosted a series of workshops reviewing the Cyber Profession. This work reviewed the IISP Skills Framework from the point of view of the role levels referenced: Levels 1 and 2: Knowledge; Level 3: Practitioner; Level 4: Experienced Practitioner – performing basic tasks without supervision, complex tasks with supervision; Level 5 – Skills Practitioner; and Level 6: Expert.

5.7.16 Functions of IA professionals are described in the following terms: i) **avoidance**: preventing vulnerabilities and exposures; ii) **deterrence**: making attack less likely; iii) **detection**: quickly spot attack; iv) **prevention**: preventing exploit; v) **mitigation**: reducing damage; vi) **transference**: shifting control for resolution; vii) **investigation**: characterizing an incident; viii) **sanctions and rewards**: punishing the guilty, encouraging effective responders; ix) **recovery**: immediate response, repair; x) **correction**: ensuring no repeats; and xi) **education**: advancing knowledge and teaching others.

5.7.17 The following CESG identified IA roles are included in the scheme, subject to continual addition: i) Security and Information Risk Advisor (SIRA); ii) IA Architect; iii) IA Accreditor; iv) IA Auditor; v) IT Security Officer; vi) Penetration Tester; and vii) Communications Security Officer. Figure 55 shows the range of possible specialisms within the IA domain, all of which are necessary in order to provide the required

level of assurance as to risk reduction and impact management for information assets.

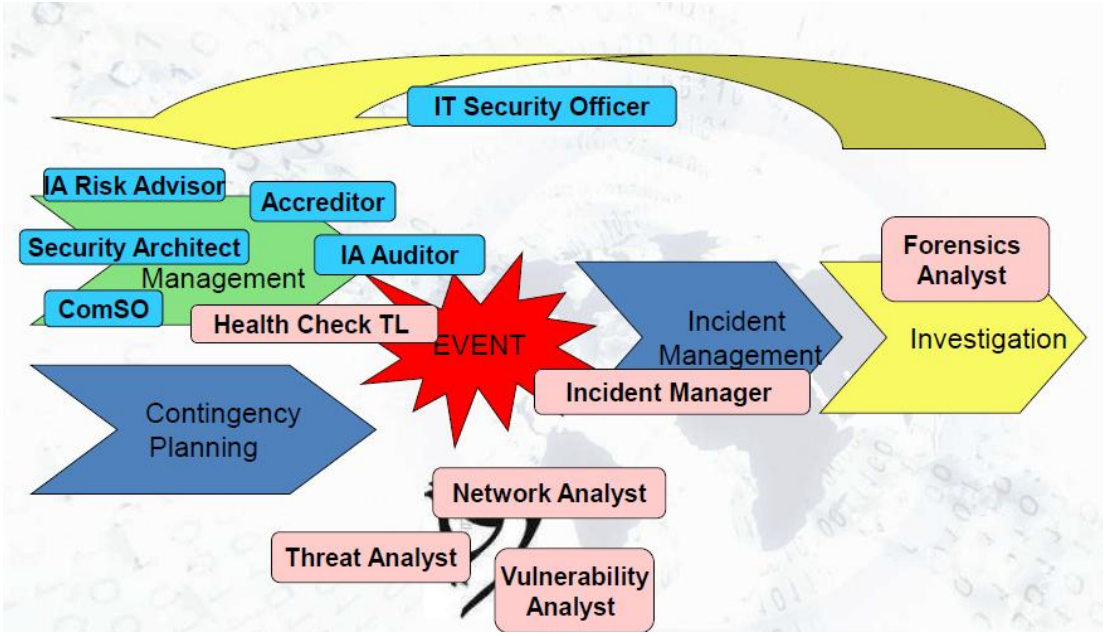


Figure 55: IA Framework Roles, Source: UK CESG (2011)

5.7.18 In 2008, the researcher was asked to review the curriculum for a newly proposed Master's Degree course (MSc) in IA at London South Bank University (LSBU), focussed on providing the skills to protect information assets. The intention was that an MSc in IA would offer strong employment prospects for graduates in many different sectors, although there was little evidence to support this on the basis of the types of roles being recruited for. Subsequently, as a result of the 2007/2008 financial crash and the resulting global recession, the number of roles available reduced significantly and the anticipated growth and maturation were not realised. A new IA Masters was designed at and for Cranfield University in 2008, but in 2009 had no students taking the course (IAAC, 2010). This reality is at odds with various research articulating a growing cyber skills crisis, though self-

interest must be considered given the context of the authors ((ISC)², 2011d; ISACA, 2014).

5.7.19 In 2011, available courses were reviewed and the difficulties of using terminology that is more akin to populist media rather than academia was raised as an issue (Furnell, 2011). Higher education institutions who design the education programmes continue to label according to what is populist (i.e. Ethical Hacking, cybersecurity) as opposed to what is principled, as academia continues to struggle to gain students in order to maintain funding and population levels. The lack of uptake of the various courses available may be because of difficulties with the terminology being used in the advertising and marketing or it may be as a result of a lack of understanding of what is covered in the course content and the value of it in terms of likely future employment.

5.7.20 The researcher created a course syllabus for an MSc in IG, illustrated in overview in Figure 56. The purpose was to evidence that a broader scope of inclusion is required in order to achieve IP. The full course content is articulated in **Appendix I, Section 10.3**.

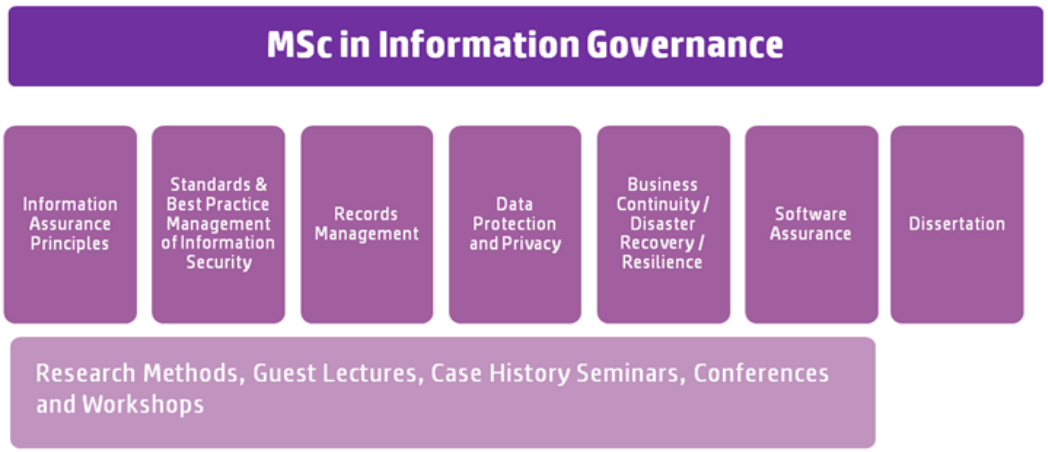


Figure 56: Proposed MSc in IG, Simmons (2011)

5.7.21 This compared positively with the MSc designed by Richardson (2012), Figure 57 below, but showed the difference in focus, raising the purview to extend across the IS domain.

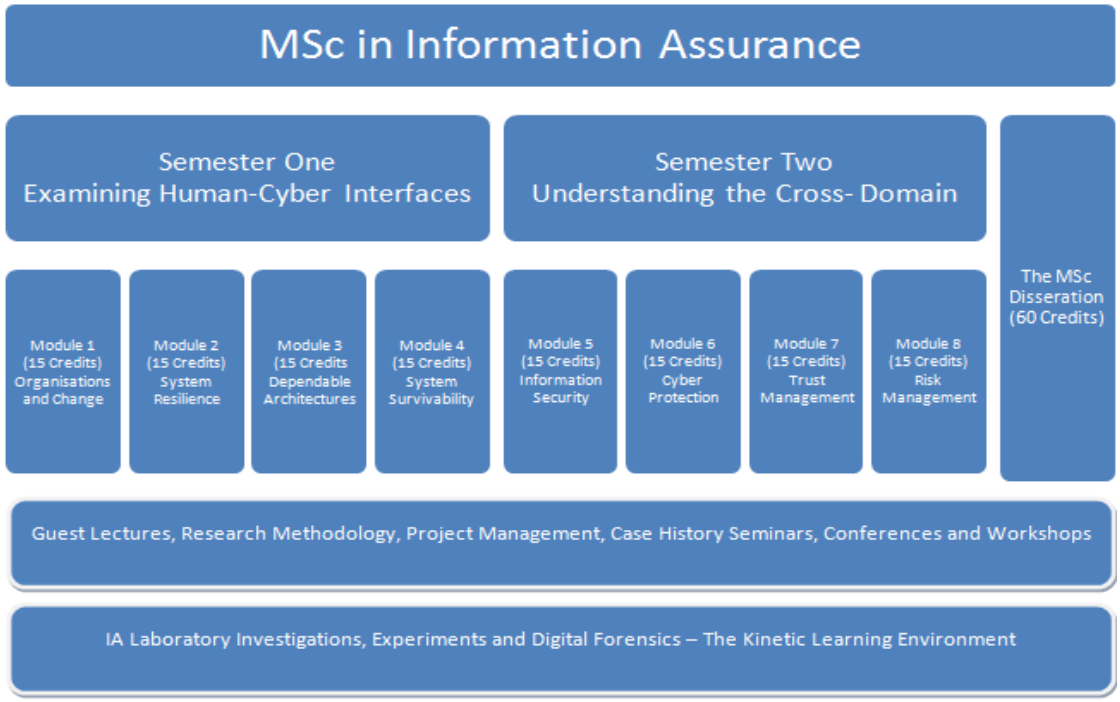


Figure 57: Proposed MSc in IA, Source: Richardson (2012, p.185)

5.7.22 In 2014, the US DHS commissioned a paper to identify best practices for the path towards professionalisation for the cybersecurity industry. The paper also explored similarities between aviation and cybersecurity (US DHS, 2014). By way of an example, the researcher engaged with a cybersecurity champion winner from the aviation industry who had never done a course in security, nor secure software design and yet was on a degree course for designing military planes for the future.

5.7.23 Chittoor (2014) electronically shared an e-Governance Competency Framework (eGCF) for Digital India, Figure 58 below in which there is no reference to security, risk or safety roles, and yet the endeavour is

to achieve e-Governance in a digital landscape. This may be forward thinking, assuming that these are functions of all roles. However, this is yet another example of overlapping, duplicative language and interlocking disciplines that lack coherence and cohesion.

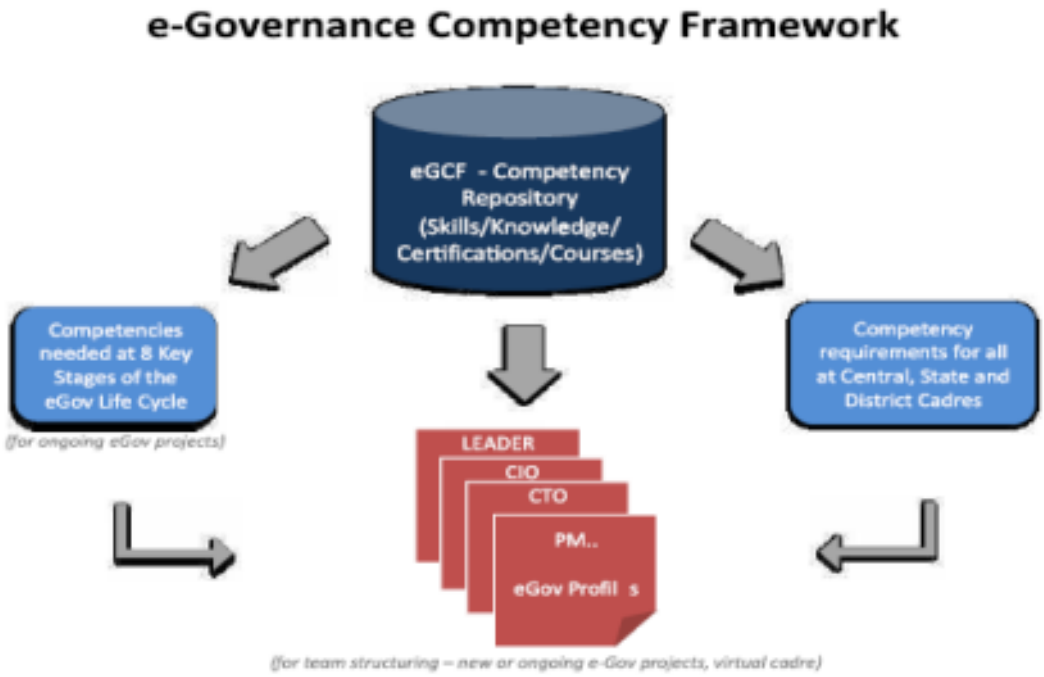


Figure 58: Digital India eGCF, Source: Chittoor (2014)

5.7.24 In 2015, the (ISC)² membership group updated their *Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees: A resource for course designers and accreditors*, ((ISC)², 2015h). The Principles sought to ensure that content would be integral to computing courses rather than a module added on. There has been notable development in this space across the UK academic institutions. However, equally the concerns are beyond that of the computing sector specifically – they are *business* issues. ((ISC)², 2015g)

5.7.25 The need for a change of view – for a holistic approach – was already identified. McBride (2007) was heretic enough to suggest that there should be no more Schools of Computing, and that a more cross-functional view was needed, in order for computing to be more divergent in thinking and delivery. These views were criticised by colleagues in the industry (Spice, 2007). Richardson (2012, p.210) developed an IA Skills Framework which contained a new holistic picture of the information domain, represented in Figure 59 below. It is missing IG, though does reference utility, similar to Parker's views (2010).

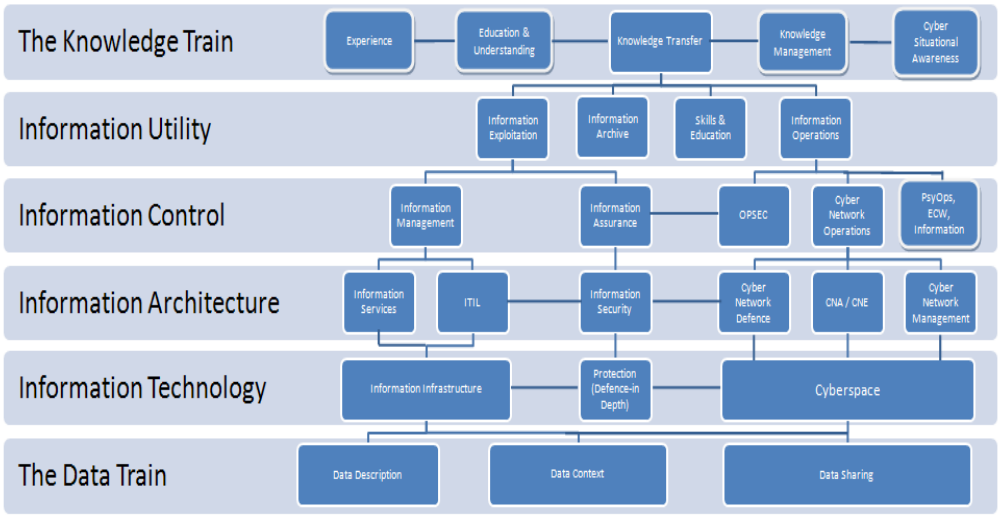


Figure 59: New Holistic Picture of the Information Domain, Source: Richardson (2012, p.210)

5.7.26 Understanding of key tenets forms a central part of educational frameworks. This has already been achieved with a number of large global private sector bodies – for example, the researcher is aware that BT and Shell have adopted the IISP and the International Information System Security Certification Consortium, Inc., (ISC)² frameworks respectively and expect relevant employees to take up membership of these bodies and undertake relevant training. This

provides greater stability, strength, and longevity to the growth of the discipline by ensuring that the necessary understanding of terminology takes place.

5.7.27 Effective delivery of holistic IA needs to advance understanding through education of leaders, practitioners and the user community in the fields of IO and cybersecurity including IM, services, exploitation, security and its assurance, critical infrastructure protection, national security and computer networks (Richardson, 2012, p.168). This communication challenge was identified a decade previously in the Harvard Business Review (Nolan and McFarlan, 2005).

5.7.28 Kovacich (1998) provided a written InfoSec Career Plan and updated this to embrace IA as the industry matured (2001). However, the responsibility is largely on an individual to manage their own career. As a career plan, seeking to reach the "C" suite (e.g. Chief Information Security Officer [CISO]) to end up in a role for, at best, fourteen months represents a challenge in the context of the ongoing skills crisis. The educational path for a doctor takes at least seven years with the expectation of ensuring career longevity thereafter.

5.7.29 The 'Inspired Careers' website, sponsored by the UK government, various companies and implemented by the Centre for Research and Evidence on Security Threats (CREST) allows the visitor to browse cyber security careers and segments a career into the categories and associate job roles represented in Table 14 below, each of which have explanatory media on the website. There is no reference to IA in the comprehensive listings.

Area	Role Types	
Trainee/ Junior	Junior Unqualified Vulnerability Assessor Technical Security Researcher Junior Programmer Security Administrator Systems Administrator (with security) Network Administrator (with security) Risk and Regulatory Trainee	Access Control Administrator NOC Operation Intrusion Analyst SOC Analyst Incident Response Centre Analyst Database Security Administrator Cyber Sales Support Researcher/Lead Generation
Practitioner	Vulnerability Assessor Practitioner Cyber Threat Intelligence Analyst Junior Malware Researcher Cyber Security Forensics Analyst PCI Consultant 27001 Auditor Accreditor Practitioner CCP COMSEC Practitioner CCP Senior SOC Analyst Intrusion Analyst	Cyber Sales Engineer Channel Marketing Manager Professional Services Marketing Manager Product Marketing Manager Product Manager Recruitment Consultant Researcher (Academia) Awareness Programme Facilitator Data Protection Officer Database Security Manager
Senior Practitioner	Penetration Tester (general) Evaluation Facility Product Tester Security Software Developer Security Architect/Senior Architect Senior Security Auditor Compliance Manager Senior Accreditor CCP Senior COMSEC CCP Security Operations Manager Cyber Incident Response Specialist Senior Intrusion Analyst	Senior Forensics Analyst Cyber Pre-sales Consultant Security Sales Executive Security Business Development Manager Technical Account Manager Senior Recruitment Consultant Security Lecturer Security Services Account Manager Awareness Programme Coordinator Cyber Security Specialist Journalist Data Owner
Principal	Specialist Infrastructure Tester Specialist Application Tester Targeted Attack Specialist Malware Reverse Engineer Principal Security Architect Principal Security Auditor Head of Compliance Information Security Manager Lead Accreditor CCP Lead COMSEC CCP Host-based Network Intrusion Analyst	Senior Cyber Security Incident Response Coordinator Network-based Intrusion Analyst Senior Database Administrator Security Product or Professional Services Sales Manager/Director Channel Account Manager/Director Principal Recruitment Consultant Head of Internal Recruitment Senior Lecturer Technical Director
Lead	Partner/Head of Division/CEO Cyber Security Professional Services Chief Information Officer (CIO) Chief Information Security Officer (CISO) Head of Division/CEO Cyber Security Software Product	Professor Head of Division/CEO Cyber Security Hardware Product Chief Technology Officer Industry Influencer Head of Internal Audit/Audit Partner

Table 14: Role titles

5.7.30 By the late “noughties”, the UK public sector had “done” IA because it had to do something tangible and measurable; the Crown cannot sue itself nor shut itself down, a power the UK Information Commissioner’s Office (ICO) has in the event of a significant data breach. The repercussions are different for the private sector, where a company may suffer a drop in share price, damage to reputation and loss of senior executives as a result of a breach.

5.7.31 Measuring the reduction in brand damage from an incident or decrease in market share due to loss of intellectual property can be difficult (Kelly, 2010). However, following the Target breach in 2014, there was a 46 per cent fall in total revenue. After a data breach in October 2015, Experian suffered their worst trading period in eighteen months – its stock price falling to its lowest level since May 2014. Similarly, in October 2015 following their public breach, TalkTalk shares dropped by over 10 per cent and by March 2016 the true costs of reparation (£60 million), including loss of customers (101,000) (Farrell, 2016).

5.7.32 Yoran (cited in Hackett, 2015) described a failure in the security industry, given the volume of technology available designed to protect organisations from breaches and loss of information and yet this is in stark contrast with the data breach reports (Verizon, Ponemon etc). The implications of Yoran's thesis are that either the technology is designed wrongly or the implementation is flawed.

5.7.33 Grupe *et al*. (2003, pp.101-110) provided an extensive piece of work reviewing options for ethical bases for IT decision making, having identified the scale of the challenge individuals faced: "... the ethical framework of IT is based primarily on the tenets of individual ethics. … suffers from sins of omission (i.e. forgetting to ask relevant questions) and sins of commission (i.e. being asked to undertake unethical actions and not being able to invoke personal ethical standards by a superior)".

5.7.34 The following list of ethical framework considerations was provided: i) "Golden rule – treat others as you wish to be treated; ii) Kant's categorical imperative – if an action is not right for everyone, it's not right for anyone; iii) Descartes' rule of change (the slippery slope) – if an action is not repeatable at all times, it is not right at any time; iv) Utilitarian Principle (universalism) – take the action that achieves the most good; v) Risk Aversion Principle – incur least harm or cost; vi) Avoid Harm – avoid malfeasance or "do no harm"; vii) No free lunch – assume that all property and information belongs to someone (intellectual property); viii) Legalism – is it against the law? Moral actions may not be legal and vice versa; ix) Professionalism – is an action contrary to codes of ethics?; x) Evidentiary guidance - is there hard data to support or deny the value of taking an action?; xi) Client/customer/patient choice – let the people affected decide; xii) Equity – will the costs and benefit be equitably distributed?; xiii) Competition – consider the degree of privacy, cost and quality; xiv) Compassion/last chance – are decision biased in favour of one group or another?; xv) Openness/full disclosure; xvi) Confidentiality – have you reduced security features to hold expenses to a minimum?; xvii) Trustworthiness and honesty – IT accountable for its actions?" (Ibid. p.105). Much of this work is corroborated by that of Dekker (2011).

5.7.35 Schou and Shoemaker (2007, p.424) referred to historical activity thus: "... a formal code for cyberspace was published as far back as 1989". The Internet Activities Board (IAB) from the Networking Group produced a directive entitled "Ethics and the Internet" (RFC 1087)

which identified the following five activities as being unethical and unacceptable: i) to seek to gain unauthorized access to the resources of the internet; ii) to disrupt the intended use of the Internet; iii) to waste resources (people, capacity, computer) through such actions; iv) to destroy the integrity of computer-based information; and v) to compromise the privacy of users.

5.7.36 There is an Institute for Global Ethics (IGE), which holds the following five Ethical Values: i) honest and truthful; ii) responsible and accountable; iii) fair and equitable; iv) respectful and mindful; and v) compassionate and caring. These two positions are shared as a starting point for consideration in terms of the IoT and the Artificial Intelligence considerations that new technologies are bringing into the industry. The BCS has a Code of Conduct, as opposed to a Code of Ethics. As identified by Raval (2012, p.9):

> A code of conduct, while acting as a compass attempting to always point at the true north, is a passive document. Only a culture of constant vigilance by leadership can make a code of conduct effective. Professionals still have to be equipped to recognize potential dilemmas and how to address them.

5.7.37 Doing security, as opposed to talking about doing security, can present new risks. Operational teams are usually attempting to achieve security whereas in large organisations there can be many different teams (Quality, Audit, Compliance, Risk, Legal, Sales, Leadership) seeking to present an outward view of the intentions – to stakeholders, to shareholders, to the Stock Exchange and beyond -

which can be significantly disjointed, particularly when it is not supported by budget and resources.

5.7.38 Consistency of performance implies the need to ensure the IA discipline exists. The term “discipline” indicates that a practice is performed consistently – and the term “ensure” implies a legal guarantee, something that Stewart (2014) was at pains to point out that InfoSec professionals needed to be careful with regards to usage.

5.7.39 IA requires discipline because procedures have to be executed in a coordinated fashion by all participants at all times. The first steps in establishing a systematic IA process is to define and document disciplined practice among the trusted individuals who access information or manage the process.

5.7.40 However, whilst disciplined practice encourages IA, it also imposes additional requirements. Workload pressures mean that people will not do everything that they should in order to be secure; they have to be positively motivated to perform those tasks. Positive motivation is essential to the IA process by initiating, directing and sustaining multiple forms of interaction. This “ensures a person’s willingness to execute a task consistently or achieve a goal, even if it is personally inconvenient” (Schou and Shoemaker, 2007, p.394).

5.8 IA in the context of Professional Identity

> *New security thinking involves a broader view of the business through the vantage point of "IA", rather than a strictly traditional "guns, guards and gates" mentality – for those who came into IA through the Physical Security route.*
> *(Dunkel, 2010)*

5.8.1 Professionals have an important role in setting societal benchmarks, putting forth the initial test cases which change legal precedents in common law. This is particularly true of the IA practitioner(s). Being a professional requires signing up to a code of conduct; committing to continuous professional development; being suitably qualified and demonstrating trusted competence. Generally, professional bodies exist to represent the interests of their members, protect the integrity of their relevant profession and raise the standards of their members' work (Warren, 2016). Sometimes they may assure the provision of quality services to the public. The ability to put professionals out of work can be perceived as an asset to maintaining trusted professional identity.

5.8.2 Professional identity is a self-concept, a constellation of attributes, beliefs, values, motives, and experiences that people use to define themselves in their professional capacity (Schein, 1978). Professional identity is therefore fluid and dependent on individuals' own subjective interpretations as they attempt to reconcile their role as part of a professional group in their own individual ways. Table 15 below summarizes five professional identity structures described by Caza and Creary (2016).

	Intersection	Dominance	Compart-mentalisation	Holism	Augmentation
Description	Individuals define themselves at the intersection of two professional identities (e.g. ITSec/ InfoSec and Cyber / IA)	Individuals define themselves by one primary professional identity to which all others are subordinated (no agreement)	Individuals define themselves in more than one professional role but identifies each profession as different points in time (identity activation is context or situation-specific)	Individuals define themselves with one holistic professional identity that encompasses all other professional identities	Individuals define themselves with multiple professional identities that are coactivated and complement, extend and enhance one another
Level of cognitive complexity	Low(est)	Low	Medium	High	High(est)
Coactivation	No	No	No	No	Yes
Integration	Integrated	Distinct	Distinct and separate	Integrated	Distinct and complementary
Reference Group	Individuals in the specific subspeciality (e.g. all nurse-midwives)	Individuals in the profession at the top of the hierarchy (this is the most valued identity) (e.g. midwives)	Individuals who are in the identity group that is salient at the time	Individuals who occupy the general superordinate category (e.g. life coach) as well as subcomponents (e.g. yoga instructor)	Individuals who occupy any of the roles the individual inhabits

Table 15: Professional identity structures, Source: Caza and Creary (2016)

5.8.3 The perception of society has an impact on the success of an industry. However, there is a lack of belief that IA occupations have sufficient well-defined and stable characteristics, in particular as a result of the interdisciplinarity and the cross-cutting themes. Individuals work in established professions and emerging professions, sometimes both. Work identities, including but not limited to professional identities, are those meanings that individuals attach to themselves in the context of work (Dutton *et al*., 2010).

5.8.4 Professional identity is a self-cognition. The more cognitively attached individuals are to their profession, the more affectively committed they will be (Caza and Creary, 2016). In the context of IA, there is a plurality of possible identities, evidenced by the complex array of duplicative and competing membership bodies – IISP, IRMA, ISSA,

ISC2, ISACA – resulting in either an intersectionist or a holistic individual. There are now cyber specific designations, from ISACA for example. Independent knowledge workers are common today – and this includes self-proclaimed IA professionals.

5.8.5 Individuals draw from personal attributes, social group membership and work roles to assign meaning to who they are and what they do in the workplace (Ashforth *et al*., 2008). In line with Benson's focus on contribution to society, individuals claim purpose and meaning as a result of the construction of their personal identity. Associating oneself with a respected profession provides pride, esteem, and well-being (Dutton *et al.*, 2010).

5.8.6 A professional may provide intangible services and the purchaser must take these on trust. Not all service provision will be successful: half of legal advocates may lose their cases in court, and some doctors will inevitably lose some patients. Strong educational background and qualifications are thus necessary, as is trust, measured by outward appearance and manner fitting the socially accepted standards of repute and respectability (MacDonald, 1995). Qualifications from education can be used to affirm professional identities – CISSP from ISC2, CISM from ISACA. Vague job titles can create ambiguity and confusion over professional identity. Safety, reliability, availability, security, and resilience are all aspects of this *trustworthiness* – also referred to as information provenance (Mansell and Collins, 2005). Clients are vulnerable because they lack the expertise to judge whether the professional that they have hired is

doing a good job; they must rely on professional ethics and competency above and beyond the pure choice of market options (Friedman, 2006).

5.8.7 There is a need to ensure that IS incorporates more reference to and understanding of the subjects contained in this thesis – those of InfoSec, IA, and IG (consider, in order: child, teenager, adult). InfoSec as an IS discipline, with someone responsible for it, has been around since the early 1970s (Desman, 2002, p.x). By 1988, it was identified that IS methodology needed to include security as a functional requirement in all stages of systems development, confirming that secure systems design requirements needed to be fully integrated (D'Aubeterre, Singh and Iyer, 2008). Once this is understood and accepted as being on a progression to maturity, all three areas can be appreciated as related to the core discipline of *IP*.

5.8.8 Discussion of industry progression was identified in Best (1996, p.53): "The profession of information science collectively and individually perhaps does not have sufficient will or motivation to advocate its own cause successfully against the much stronger commercially driven pressures of the IT professions". The importance of the IM theme is undiminished, more particularly with the emergence of the Big Data agenda and discussions about Data Lakes – another new industry term denoted to signify the resting volume of data available.

5.8.9 The **Chief Information Officer** (CIO) is a 30-year-old role at this stage and yet even 20 years ago, was suffering from political battles with the Chief Operations Officer (COO) (Best, 1996, p.148). The researcher

contends that core to this dynamic is an understanding of the constituent parts, in line with the following:

> We can manage the technology (most of the time) and the organization of knowledge (ditto), but we are not very good at dealing with people and organizations in this context. We lack the necessary methodology for investigating and analysing these situations, and we lack proper understanding of the fundamental principles of individual and social behaviour involved in information use. As pointed out earlier, there is a serious need for more research in this field (Ibid. p.135).

5.8.10 Despite their title, **CIOs** are, largely, *only* responsible for technology infrastructure and *not* the information itself; they typically find themselves more concerned with updating network configurations and ensuring cloud architectures are in place than with policy issues affecting data. This has left a gap into which a Chief Digital Officer (CDO) has been inserted, which is a cost drain and shows a lack of understanding and maturity by those already in the available roles.

5.8.11 The **Chief InfoSec Officer** (CISO) has a responsibility to spend their time advising the organisation they serve about the risks to information from identified vectors and provide guidance on appropriate risk reduction mechanisms. Yet largely the CISO cadre are still technically focussed and lack education and awareness across the breadth of the information domain, particularly in terms of compliance understanding, regulation, legislation, protection, preservation and overall IG.

5.8.12 The UK Public Sector **SIRO** role was designed to address IRM. There is no specific private sector equivalent, though some organisations have a **Chief Risk Officer** (CRO). However, the dominant narrative between the two roles can be worlds apart; the risks identified may be different; the appetites are not matched; and the thresholds are not equal. This is not a level playing field; even the existence of the ISO31000:2009 international risk management standard has not consolidated views in this domain.

5.8.13 A **Physical Security** practitioner may identify IA in terms of security passes and access to buildings.

5.8.14 A **Network Administrator** might identify IA in terms of permissions, rights, and passwords.

5.8.15 An **InfoSec Professional** tends to identify in terms of unauthorised access to electronic systems, hackers, firewall management, etc – in other words, in technology issues and solutions, across the technology space, rather than upwards and outwards across the organisation, embracing the information assets at a management and director level. Membership of IS Security Association (ISSA) and (ISC)², BCS Chartered IT Professional body and the IISP are all likely. Most security professionals are members of American owned membership bodies and are therefore influenced by the newsletters and magazines that review the themes and influence the thinking.

5.8.16 A more mature **InfoSec Professional** tends to understand the Five Pillars as an overlay on the technical issues, but their role is broader. There is a *lot* of distorting of the definitions in job descriptions. The

role had been described as that of an ISSO – an IS Security Officer in the original 1998 edition from which Kovacich updated the description for the 2006 publication (Kovacich, 1998).

5.8.17 **IT Security** practitioners would define it in terms of firewalls, intrusions detection and prevention, viruses and hackers, vulnerability assessments and a whole host of directly technical elements.

5.8.18 An **IG** practitioner – who has a background of broader policy and legal understanding – would have the InfoSec CIA triad central to their view - but would also include Accessibility, Usability, and Authenticity – as some of their key drivers with regard to Information Access. They operate with a wider understanding of information-based legislation such as the Data Protection Act and Freedom of Information Act. For an IG practitioner, Records Management and IA are inter-connected.

5.8.19 An **IM** practitioner knows to include Data Quality and frames their activities to include Knowledge Management.

5.8.20 A **Records Management** practitioner knows that there will be times when a great deal of store will be placed on the accuracy, timeliness, and availability of core corporate records to evidence acts undertaken, agreements reached and decisions made, none of which will be possible without many of the elements possible through IA being in place. Membership of the Information and Records Management Society (IRMS) is likely. For many years, this group was the Records Management Society but renamed in 2010 to reflect how central the "information" element is to the success of Records Management – as

is also the case with (*information*) security and (*information*) assurance.

5.8.21 An **Audit** professional will be familiar with the terminology of GRC, controls, and countermeasures across the whole space. Internal Auditors have a role in providing *assurance* that policies and procedures are being followed on strategic, operational, financial, and compliance objectives addressing laws and regulations, and that the internal controls in place are adequate to mitigate risks. Equipped with an in-depth understanding of the organisation's culture and ethical environment, they are positioned to bring great value to the entire process of effective governance, risk management, and internal control through their insight into the organisation; the objectivity with which they view the organisation's culture, system of internal control, and risks.

5.8.22 For an **IT Audit** practitioner, membership of ISACA is likely. However, to add to the confusion, IA for an Auditor will stand for Internal Audit, whereas within the same organisation, IA can also denote Information Architecture and Identity Assurance. The IA practitioner and the Auditor come together around the topic of control. They may not agree on the method selected to establish the control but the risk concerns need to be understood from the same terminology standpoint. Both disciplines need to work together in responding to Audits too. The IA practitioner needs to know that they have the evidence available and can present it in an appropriate manner without creating greater risk for their organisation; whilst the Audit

Professional needs to be able to absorb and understand the evidence provided, within the context of the business specifically, rather than necessarily through the lens of wider expectation (Bell, 2010, p.34). IT Auditors work at the intersection between IT systems and the people who specify, develop, implement, use, manage and maintain them, and thus need to be competent and comfortable with a broad spectrum of issues (Hinson, 2007).

5.8.23 Other roles and terms exist. McFadzean's Literature Review (2005) sought to identify useful frameworks for aligning IA with corporate strategy. McFadzean referenced the work of Kovacich (2001) who had already seen the need to merge the roles of the Corporate Security officer and the IS Security officer to a more senior position, perhaps called the Corporate IA Officer. The purpose of the role would be to "develop, implement, maintain, manage and administer a corporate-wide IA programme to include all plans, policies, procedures, processes, assessments and authorisations ready to protect and defend the corporation's information and information systems, regardless of its location and environment" (Kovacich, 2001, pp.302-307). This followed on from the use of the term "information guardians". This was a more solid paper than that previously written by the author and colleagues (Birchall *et al*., 2003) as the maturation of the thinking around IA was clearer to see and the definitions were more accurate and appropriate. "IA could be said to represent a migration from a *preventative* approach to an *enabling* approach" (Birchall *et al.*, 2004, p.7).

5.8.24 In 2011, the UK's Data Protection Forum (DPF) signed an undertaking with the International Association of Privacy Professionals to allow for cross membership. Quigley (2008) produced an extensive encyclopaedia of reference material on information ethics and security, without a single mention of IA. The encyclopaedia is not lacking as a result of this omission. This highlights that ethics and privacy are seen as being linked (Viscarolasaga, 2009, p.11) – and that professionals need to understand Data Protection (DP) in Europe in the context of privacy worldwide. However, this is not a group that current IA practitioners would naturally migrate towards.

5.8.25 With this number of possible perspectives, the lack of a formal professional IA body in the UK means that practitioners are often creating their own definitions and harnessing them at the expense of an available and defined reality. The issue of definition continues to be important if it is accepted that the skills required from future IA professionals need to be taught by current academia through the available curricula.

5.8.26 Barwise (2013) highlighted the importance of understanding the meaning of the terminology used in the context of the CIO, CISO and CTO roles and provided a steer as to who best to represent the concentric circles of overlapping domains. The scope is nested in the same way as are the established disciplines of IA, IS and ITS, represented in Figure 60 below. Complementary expertise is required between the domains and sharing of knowledge should lead to success.

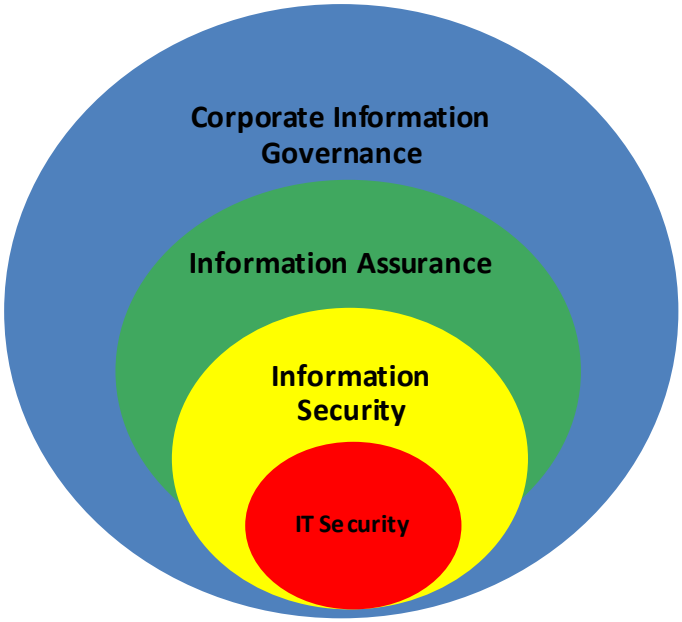


Figure 60: Corporate IG, overlapping domains, Source: Barwise (2013)

5.8.27 The lack of a common curriculum that all IA students could take diminishes the acceptance of the profession. There is no consistency in what is taught. All IA graduates are not created equal. Coming from a business background ensures the IA professional is well-versed in relevant policies and procedures while those with engineering backgrounds will have a more technical, architectural perspective. The discipline of IA is relatively young and maturity will not be guaranteed without academia supporting the transition required through more directed teaching.

5.8.28 Wylder (2004, p.28) pointed out that skills change over time:

> The type of person chosen to fill the role of security manager may change depending on where in the life cycle an organisation falls. In the early phases, a limited-function position emphasizing technical and administrative skills may be appropriate. Later it

may be necessary to redefine the job to bring other skills into play.

5.8.29 Blyth and Kovacich (2006, p.153) pointed out that:

> The [*insert relevant title*] who does not look ahead at the trends in society, technology, business, global competition, criminal justice systems, crime and any associated rapid changes will have a stagnant [*insert interchangeable InfoSec or IA*] program that fails to meet the needs of the business or government agency.

5.9 Conclusions

5.9.1 The findings of the research showed that business, academia, and government do not fully understand IA, neither in definitional terms nor in implementation requirements. The lack of adherence to the available lexicon and taxonomy, and the lack of an international standard for IA conspire to continue the compounding of confusion, and the lack of progression of IA as a successful profession. **[15ES, 35F, 57S, 62S, 69S]**

5.9.2 As observed in the private sector case study **[CS2]**, operating assurance in silos (including risk management, internal audit and compliance) has led to leaders being unable to trust the value of business intelligence provided to them. Ill-disciplined governance efforts exacerbate these problems and often lead to false comfort and inadequate oversight. It is a key industry challenge that much of what is known about by IA professionals cannot be discussed openly due to the likely increase in risk and the resultant decrease in share price that could occur.

5.9.3 Survey respondents and PAR in the public sector case study **[CS2]** identified that the concentrated focus on IT often causes management, when faced with almost every problem, to demand another IT solution. Corporate business is not yet in the information centric mindset which can be developed into one which embraces IG. There is a long way to go before the level of sophistication is sufficient enough to embrace this. **[39FE, 48S, 67S]**

5.9.4 Through the Literature Review, it was already identified that the IT industry is confused between governance and management (Weill and Ross, 2005). Repeatedly, this researcher has come up against these misconceptions. One survey respondent articulated that "The words governance and management are somewhat interchangeable – it's mainly based on where you sit in the food chain". **[50S]**

5.9.5 Survey respondents alongside literature review also identified that the pace of change brought about by the Internet – and the IoT - has made society post-Euclidian and post-Newtonian; consequently, decision-making processes have to change. **[34F, 35F]** This requires the combination of a number of elements - an *Idea* (the Truth or "Aha" moment), a well formed, well-educated *Team* (Execution), a *Plan* (Business Model), *Funding*, and *Timing*. Research has shown that the greatest of these is Timing (Gross, 2015).

5.9.6 The research identified that attributes of a profession include: i) a body of knowledge, ii) ethical guidelines, and iii) a professional organisation with a growing set of published papers and best practices (Cox, 2010, p.7). Professionalisation as a process involves the creation of: i)

group norms; ii) qualifications (of which there are many); iii) codes of conduct / ethics (again, there are many); and iv) a professional body to oversee the conduct of members of the profession (this does not exist).

5.9.7 As identified by the survey responses, the PAR case studies and through industry engagement, the researcher has identified that there is no unifying narrative of an IA profession as a result of the widespread roles and functions incorporated, alongside the multiplicity of professional identities. **[46S, 60S, 74S]** In the UK, there are no specific IA bodies, save for IAAC which is a voluntary rather than a professional membership body. However, to introduce a separate IA professional membership body into the existing domain may not be the best approach, given the areas of coverage of the existing longstanding groups, their membership numbers and global recognition. Conflicting approaches identified throughout this research are indicative of gaps in the IA professionalism agenda. **[69S, 76S]**

5.9.8 Through the lens of professionalisation, reviewing professional knowledge, professional identity, IA understanding, professional membership, and exposure to the industry, the researcher has considered whether an IA professional can be a cybersecurity professional and, conversely, whether a cybersecurity professional can be an IA professional. The foreground understanding of IA professionals is rested within the dominant narrative of InfoSec, with an acceptance that cybersecurity is the prevailing term being utilised. This is creating multi-identity challenges.

5.9.9 Organisations, in all sectors, are left confused, considering whether the professional identity of an IA professional is different from an InfoSec professional is different from a Cybersecurity professional. In austere times, organisations cannot be expected to support so many fractured disciplines, with multiple affiliations, membership fees, certifications, and codes of ethics.

5.9.10 Trustworthiness and the constituent elements of trust were key themes that were identified from the survey research. **[47S, 52S, 56S, 57S, 69S]** Trust characteristics include *reciprocity* – the ability to demonstrate mutuality of governance measures; *clarity of responsibility and liability*. These are important areas in organisational dynamics with the volume of outsourcing and off shoring, where third parties are performing the greater volume of actual business processing and teams need to have known and understood the legal implications of these activities and to have agreed baselines of culture and expected behaviour, irrespective of the prevailing culture. *External demonstrability* requires the ability for each participating entity to provide the necessary external representation to meet expectations and support the required confidence of stakeholders. This is most keenly felt in the financial sector though is equally prevalent in the health sector. **[CS2]**

5.9.11 The survey respondents identified many cross-cutting themes – product assurance, quality assurance, project assurance – achieving IA should be a normal part of business outcomes in the information age. These are reliant on both the existence of and the maintenance

of *quality* information. Quality, in security terms, can be expressed as a factor of accuracy, trust, and integrity. Given the breadth and scale of what needs to be assured, the volume of "cyber" rhetoric is overwhelming. **[20F, 39FE, 46S, 48S, 60S, 67S, 74S]**

5.9.12 In the private sector case study, it was observed that corporate business can take the view that neither information nor records management depend upon a threat to do the right thing. Acceptable *business* risk, not just acceptable risk, is what needs to be striven for. **[CS2]** This was the stance taken by the TalkTalk CEO, following their third breach in a year (in October 2015), in claiming that encryption was not mandated in legislation for data in transit or at rest (Zorabedian, 2015).

5.9.13 From Cadbury (1992) **[72S]**, through Turnbull (ICAEW, 1999) **[84F]**, through Enron (Turnbull, 2002) **[84F]**), through the financial crisis of 2007 onwards, there has never been so much information available and accessible and yet there are organisations behaving as if implementation of long established security frameworks, controls and safeguards is optional rather than required. IP related legislation exists though historically it has lacked the ability to sufficiently punish proven misdemeanours. EU Data Protection Authorities will have the capability of imposing increased fines on those who infringe existing guidance based on the EU GDPR principles. These penalty structures may provide sufficient incentives to result in behavioural change in terms of data collection, processing and security. In the researcher's experience, there is no evidence that this will be the immediate

response. Corporate governance needs to dictate a more appropriate approach. These activities must become part of a wider organisational IP UCF. **[14F, 41E, 46S, 60S, 74S]**

5.9.14 The empirical evidence gathered through this study produces a tautological conclusion. Breaches will continue to be experienced for as long as IA is not successfully achieved, as a result of the barriers identified throughout this research. Greater IA understanding, will lead to more controls being effectively implemented to reduce risk of breaches and their impact. This change must be realised in the wider context of organisational IG, requiring deeper knowledge and ongoing education of InfoSec professionals, specifically. Stronger alliance is required across all departmental disciplines, including: HR, Legal, Procurement, Sales, Marketing, etc., in order to protect the IP requirements end to end throughout the lifecycle, from creation through to destruction or preservation. The real challenge faced is not in defining the goal but one of organisational dynamics, politics, influence, credibility, etc. IA initiatives have to move from being the necessary evil to being a business enabler. **[39FE, 48S, 67S]**

5.9.15 During the course of this research, it has become evident that IA has much in common with existing governance frameworks - management, corporate etc. Following iterative discourse analysis of the survey responses and synthesis of the combined evidence and literature review, the importance of IG in the context of IP was identified by a number of respondents, **[20F, 58S, 60S, 71S, 77S, 81S]**, alongside the experience gained through the PAR activities.

5.9.16 It was in this context that utilization of a grounded theory led to the realisation of a step change being required from the existing GRC ontology. In the researcher's opinion, GRC requirements need to be seen as intrinsically the same across all sectors, with *information* being the fuel that maintains the engines of business, commerce, government, power etc. **[77S]** Frameworks which are able to visualise and express non-tangible assets are valuable data points. Research which compares InfoSec governance frameworks with environmental governance frameworks has much to benefit differing communities (Coles-Kemp, 2008).

5.9.17 Thus the researcher developed a roadmap for the future of IA, resulting in the framework i3GRC™ (Integrated and Informed Information Governance, Risk, and Compliance). As new pieces of information were made available, the search for a solution continued to change direction. This was in keeping with the Keen's entreaty (1980, p.18):

> Let us make sure we keep a few philosophers, historians, general systems theorists and social activists within our network: even if only to write useful survey papers. Research is the professional core of a discipline, but for it also to be the intellectual core, we need to think about research, not just do it.

5.9.18 For the theory building, use of the IT GRC label was discounted as the continual reference to IT skews the intentions and switches off the intended audience. Enterprise GRC (eGRC) is another label in circulation. This is a central tenet of i3GRC™ - that the scope is

enterprise-wide. In January 2015, distillation of the theoretical elements of this study resulted in the encapsulation of the requirements – *integrated and informed information governance risk and compliance – i3GRC™* and the visualisation of the supporting graphic. This acronym was registered as a trademark in March 2015 and was confirmed as a unique mark, with no detractors, in May 2015.

5.9.19 Chapter 6 answers the fourth research question - Is it possible to produce a framework suitable to support the route from IA to IG? – articulating the framework review that led to the distillation of the constituent elements of i3GRC™.

6 i3GRC™ – INTEGRATED AND INFORMED INFORMATION GRC

6.1 Introduction

> *Powerful communication between people plays a critical role in a company's bottom line. Without it you're toast!* Ampoma (2012)
>
> *"The art of communication is the language of leadership."* Humes (2003)

6.1.1 Following the grounded theory exposition in Chapter 5, consolidating the data and identified phenomena from the study, this chapter addresses the final research question: Is it possible to produce a framework suitable to support the route from IA to IG? The research evidence supports the researcher's contention that repositioning and realignment of IA is required in order to ensure its' survival, or it must be consigned to the history books. The Researcher is advocating alignment with IG in order to best influence the required IP outcomes. Management of complex adaptive systems is ultimately the requirement in order to achieve IP, reducing the likelihood of risk from cybercrime. This requires process standardisation in order to ensure repeatability and consistency of results, creating a UCF. Executive level commitment is vital – "there is no such thing as too much accountability" (Nolan and McFarlan, 2005, p.10).

6.1.2 The constituent parts of i3GRC™ require: integrating the compliance evidence with the external validation and verification; the ability to provide visible commitment to industry standards, applicable legislation and regulation; and the results from periodic self-audits that feed into corrective action plans (CAP) where required, with

appropriate sharing with stakeholders on a need-to-know basis. The approach needs to be test once, publish once, share as applicable – rather than the often exhausting and certainly resource draining multiple, duplicative audit efforts being carried out to evidence compliance with a multitude of regulation, legislation, and industry standards.

6.2 Existing Models

6.2.1 Work produced in 2009, during an IG programme conducted for EURIM (now the DP Alliance – a conservative political group supporting government ministers in understanding policy evaluation issues), aligned with industry activity identifying stakeholders with conflicting objectives for whom the imperative was to work together to address each of the goals within an IG framework (Kofsky, 2011). The resulting model, shown in Figure 61 below, was produced from a UK Government, information centric standpoint.

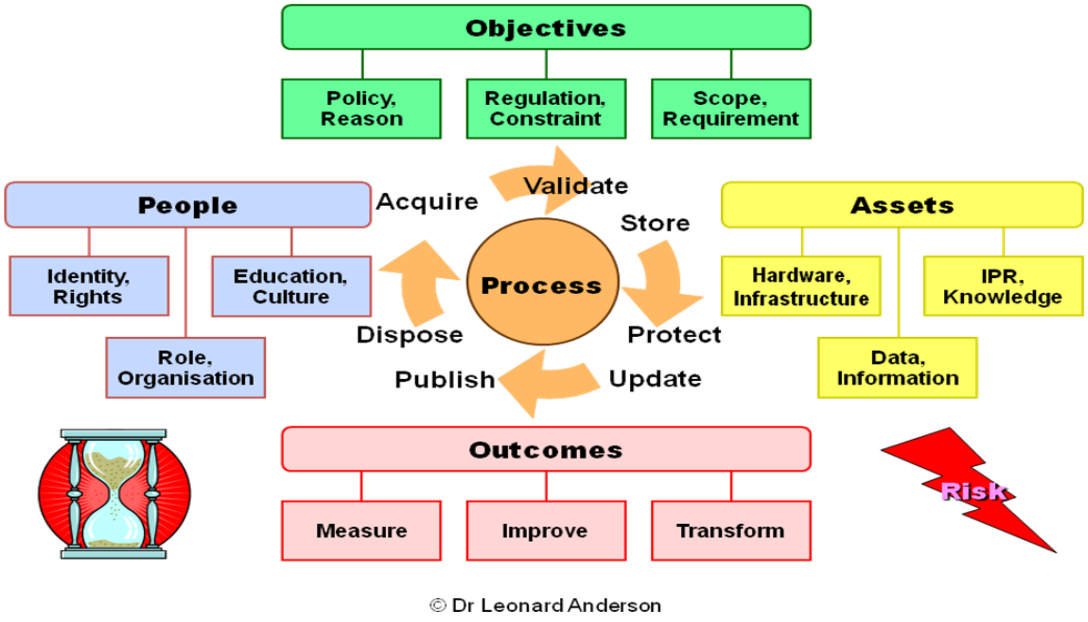


Figure 61: Information Landscape, Source: Anderson (2009)

6.2.2 Also in 2009, the OCEG (2009a) produced the "GRC Capability Model", for implementation of a *federated* GRC (within the business community), as represented in Figure 62 below:

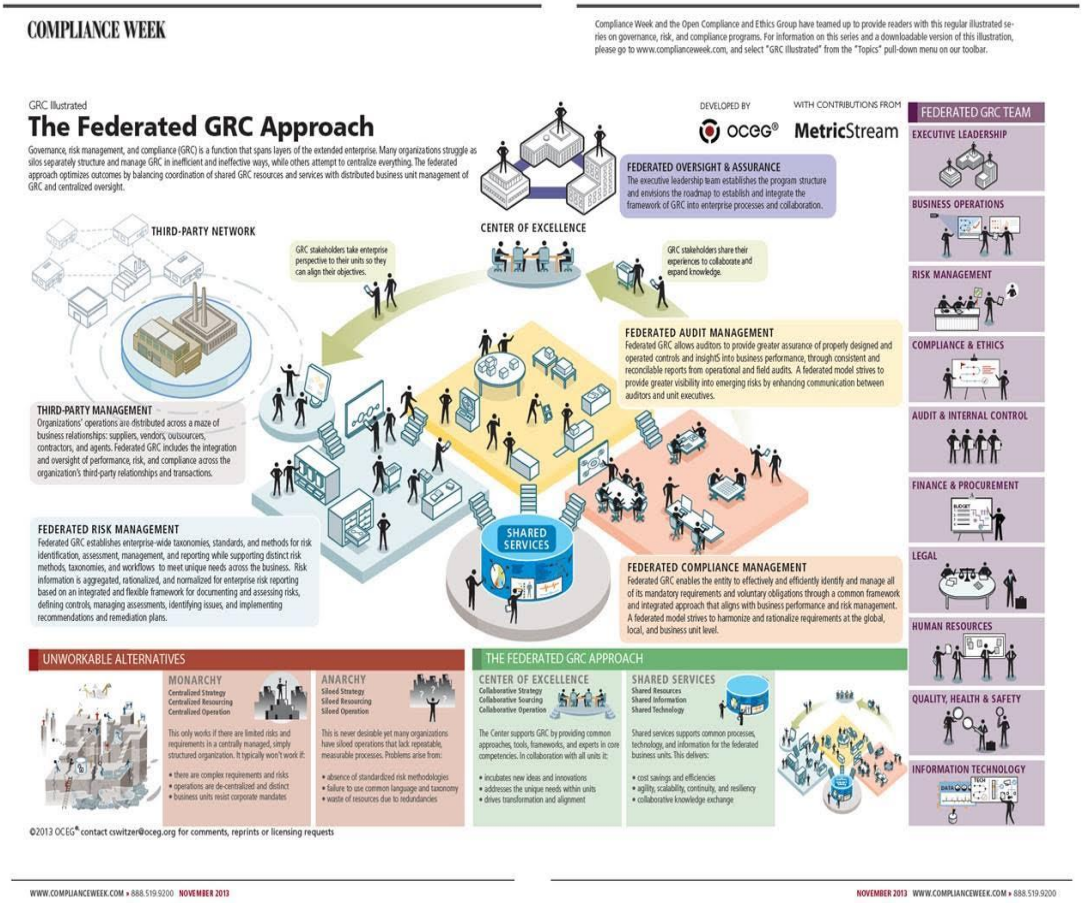


Figure 62: GRC Capability Model, Source: OCEG (2009a)

6.2.3 Racz *et al*. (2010, p.11) produced a model to represent business operations managed and supported through GRC in a strategic context; advocating the use of their frame of reference for future research of integrated GRC.

6.2.4 This has been subsequently reproduced, without attribution and enhanced, in Figure 63 below (Wright, 2011).

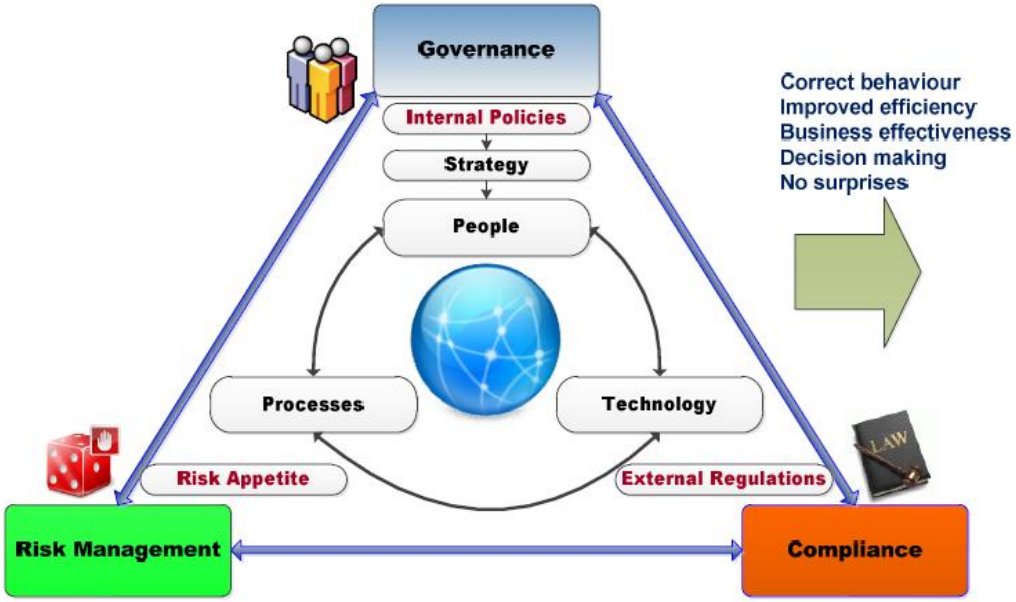


Figure 63: Frame of Reference for Integrated GRC, Source: Racz *et al*. (2010, p.8)

6.2.5 IBM has been advocating information integration for over a decade (IBM, 2005), the terminology maturing to *Information Integration and Governance* (IIG) in the 21st century. Figure 64 shows the IBM maturity path for achieving IIG, moving Big Data from Operational to Strategic.

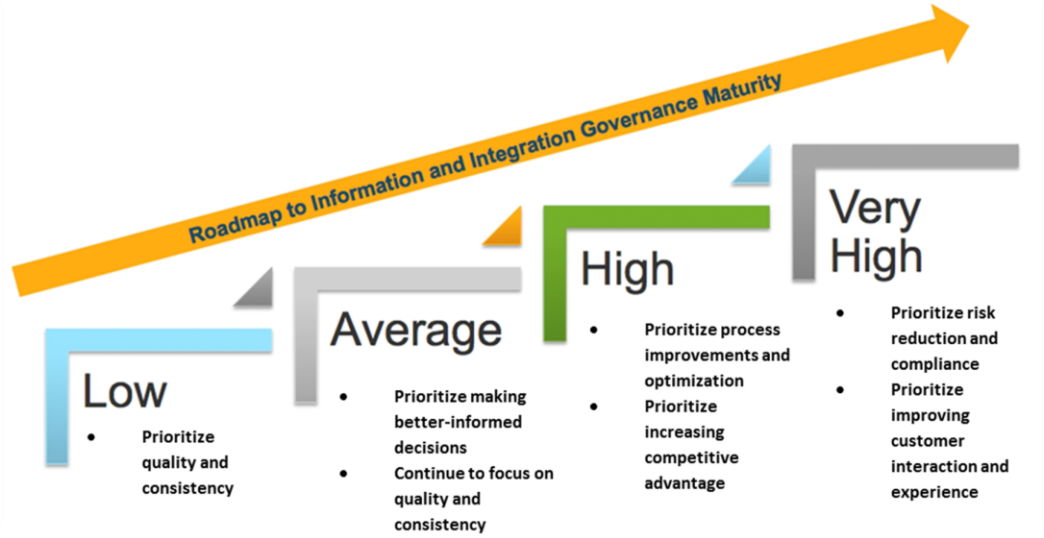


Figure 64: Mature IIG, Source: cited in IBM (2013, Slide 16)

6.2.6 The work undertaken by Vicente (2011) also identified the need for **integration**, as represented in Figure 65 below, presumably being conducted in parallel to that of Racz *et al*. (2010).

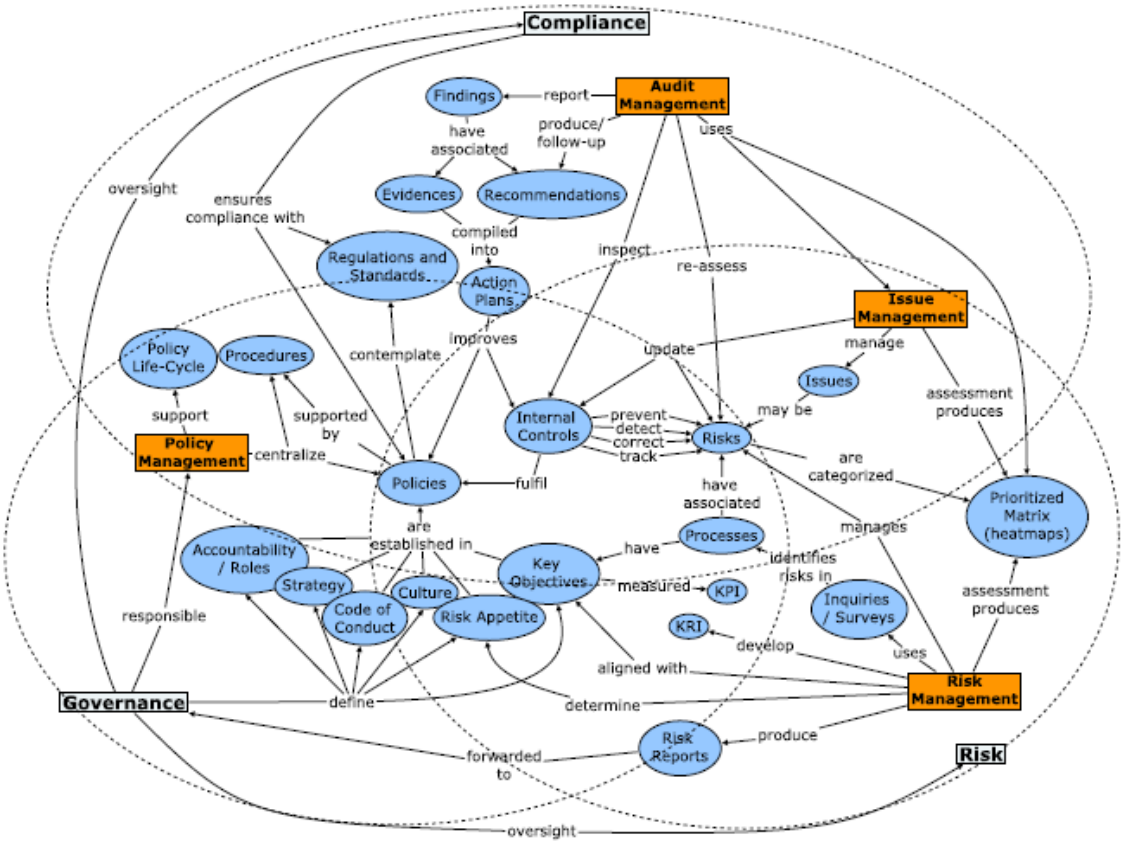


Figure 65: Integrated GRC Conceptual Model, Source: Vicente (2011, p.28)

6.2.7 Having reviewed the volume of available data points, the task, through the Grounded Theory, was to identify new ways of addressing IP through the lens of systems thinking. Senge (2002) addressed the discipline of systems thinking thus:

> Systems thinking is a discipline for seeing wholes. It is a framework for seeing interrelationships rather than things, for seeing patterns of change rather than static "snapshots" ... the subtle interconnectedness that gives living systems their unique character.

6.2.8 Figure 66 below encapsulates the layers of activity required to be integrated, alongside the areas that employees, managers, and leadership need to be informed about, all of which have *information* at their core (Iron Mountain, 2014, p.11).

Figure 66: A Practical Guide to IG, Source: Iron Mountain (2014, p.11)

6.2.9 The private sector needed to apply transformational thinking with regard to integration and reduction of complex structures in order to streamline data collection, evidence gathering, and overall IG. However, the incremental improvements to the status quo that have been systematically implemented year on year appear not to be sufficiently appropriate given regular failures in InfoSec and privacy concerns. By implication, there must be other impediments, including corporate

culture and social environment, which are contributing to the continuing difficulty in this area and therefore a broader sweeping organisational change is required.

6.2.10 The OCEG continued to invest in maturing their framework, upgrading the original GRC model to include Principled Performance focusing on *integration*, as shown in Figure 67 below.

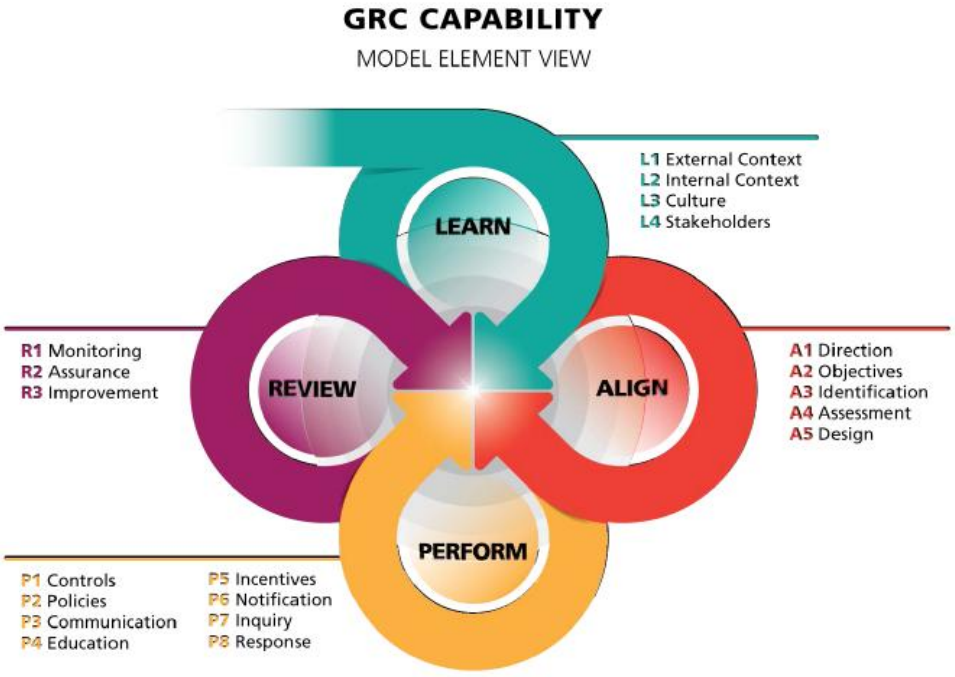


Figure 67: GRC Capability Model Element View, Source: OCEG (2015b, p.16)

6.2.11 Much work has been done in the public sector representing the large scale transformation that has been taking place during the early 21st century, as represented by Table 16 below, comparing between Command and Control Thinking and Systems Thinking:

Command-and-Control Thinking		Systems Thinking
Top-down, hierarchy	PERSPECTIVE	Outside-in system
Functional specialisation and procedures	DESIGN OF WORK	Demand, value, and flow
Separated from work	DECISION-MAKING	Integrated with work
Output, targets, activity, standards: related to budget	MEASUREMENT	Capability, variation: related to purpose
Contractual	ATTITUDE TO CUSTOMERS	What matters?
Contractual	ATTITUDE TO SUPPLIERS	Cooperative
Manage people and budgets	ROLE OF MANAGEMENT	Act on the system
Control budgets, manage people	MANAGEMENT ETHOS	Learn through action on the system
Reactive, projects	CHANGE	Adaptive, integral
Extrinsic	ASSUMPTIONS ABOUT MOTIVATION	Intrinsic

Table 16: Organisational Command and Control vs. Systems Thinking, Adapted from Vanguard Consulting Limited (2001) and Seddon (2008, p.70)

6.2.12 Thinking about IA in complex systems terms means considering achieving IA as an emergent property of systems – like safety (Cook, 2000). Complex systems are intrinsically hazardous systems. If risk did not exist, controls would not be required. Complex and large are *not* the same thing in the context of systems. A complex system can still be a small system. A complex system needs to be capable of being used by simple folk, rather than a simple system that is too complicated to use. Depth of understanding is required in order for complex system creation to be successful.

6.2.13 Complex systems are necessary for running large businesses, *not* spreadsheets – particularly in order to generate actionable intelligence. From the available data, analytical skills are required in

order to generate the appropriate, proportionate and most beneficial actions. These are relatively new skills within the InfoSec community.

6.3 New Framework

6.3.1 This research has followed a similar analysis approach to that of Coles Kemp (2008), Gericke *et al.* (2009), Racz *et al*. (2010), Vicente (2011) and Powell *et al*. (2010). The latter identified the need for the use of an "IA Range Framework" to test and evaluate (T&E) interconnected systems to ensure the effectiveness of implementation. However, the researcher contends that this was previously addressed by the Orange book (UK HM Treasury, 2004).

6.3.2 The requirement for future research of integrated GRC using the Racz model is the starting point of i3GRC™. The whole process has led the researcher to believe that what is required is a holistic strategy for using and managing information to meet business objectives.

6.3.3 IG provides this by assuring the quality of content and data, maximising its value and ensuring its security and privacy throughout the lifecycle. Combining IA, IG and GRC achieves i3GRC™ – integrated and informed GRC.

6.3.4 i3GRC™ was borne out of an observed need to implement a unified IG framework on a large, organisation-wide scale. i3GRC™ can be viewed as a framework within which to articulate an IP conversation. i3GRC™ is an instance of an ontology for addressing IA from an enterprise perspective.

6.3.5 Figure 68 presents the graphic demonstrating the reference model for i3GRC™ which has been implemented in the private sector case study [**CS2**], forming an original and significant piece of research.

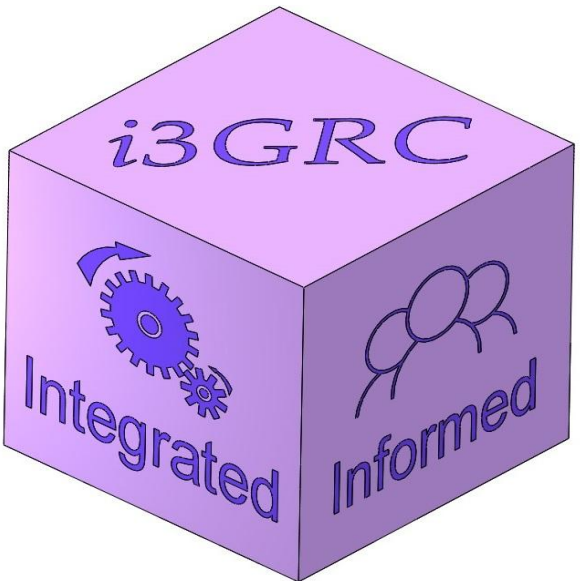


Figure 68: i3GRC™ Reference Model created by Simmons, 18 January 2015

6.3.6 The i3GRC™ framework contains the following elements: i) setting corporate objectives; ii) identifying boundaries (legislation, regulation, industry standards, contractual requirements etc); iii) assessing *all* risks; iv) putting controls in place to reduce the identified risks to an acceptable level (*proactive;* v) monitoring all systems to ensure that the implemented controls are operating effectively (*detect and check*); vi) *responding* to all incidents, and to all other stimuli, both internal and external; vii) *evaluating* framework effectiveness through self-assessments, internal audit, external [regulatory] audits; vii) *improving* the framework, adopting the Principled Performance ethos, ensuring that all of the information feeds [inputs] are used to continually improve the outputs; and viii) *communicating* constantly, positively, collectively and universally.

6.3.7 i3GRC™, therefore, requires vision to ensure that all organisational information sensors (from PPT) are being fed into the framework wherever possible. The benefits of operating in this manner are manifold, including: i) provision of a central repository of all system and audit evidence; ii) improving decision support through a holistic and integrated view of risk and compliance posture; iii) consistently tracking of all Issues – spanning Audit, Compliance, Security, Risks, Exceptions to Policy; iv) more successful and faster Audit completion (Internal and External); v) ease of reporting - Executive Dashboard capability significantly increased – multiple *Dashb*oards reduced and consolidated; vi) increased operational effectiveness; vii) increased completeness and accuracy of available information through automation; ix) ease of use for every level of employee – across decision making, prioritisation, issue ownership etc; x) reduced effort associated with manual self-assessments by integration of automated host scanning data; xi) standardized and automated Security Officer functions allowing them to focus on higher value activities; xii) evidence capture for compliance with confidentiality, privacy and data protection assurance requirements; xiii) Incident Management reporting end to end – assisting in breach management, external communications management, reparation, and resilience; xiv) improved information asset handling, reducing multiple asset sets, consolidating into one repository; xv) provision of backup evidence and support; xvi) storage of Business Continuity Plans, alongside Business Impact Analysis (BIA) following correlation with existing Risk

Registers and Corrective Action Plans to reduce duplication of effort; xvii) collation and management of Access Control configuration information, user identification and authentication is maintained; xviii) Storage of Certificate Management information to ensure appropriate renewal; and xix) Appropriate records management within the system, access control is managed, separation of duties occurs and information is segregated on a need to know basis.

6.3.8 The US Military IA Policy Chart, which has been subject to regular updates, provides an end to end view of the scale of the requirements and operational links, highlighting the plethora of available related NIST standards and guidance. Note, in keeping with the researchers' concern regarding nomenclature, and the imminent demise of the usage of IA, in June 2017, this was relabelled as the "DoD Cybersecurity Policy Chart". From the perspective of a practitioner, the framework structure is applicable more widely than its intended military audience (US DoD, 2017). Taking this inspiration, the scale and scope of the documentation required to be housed in the i3GRC™ repository is represented in Figure 69 below.

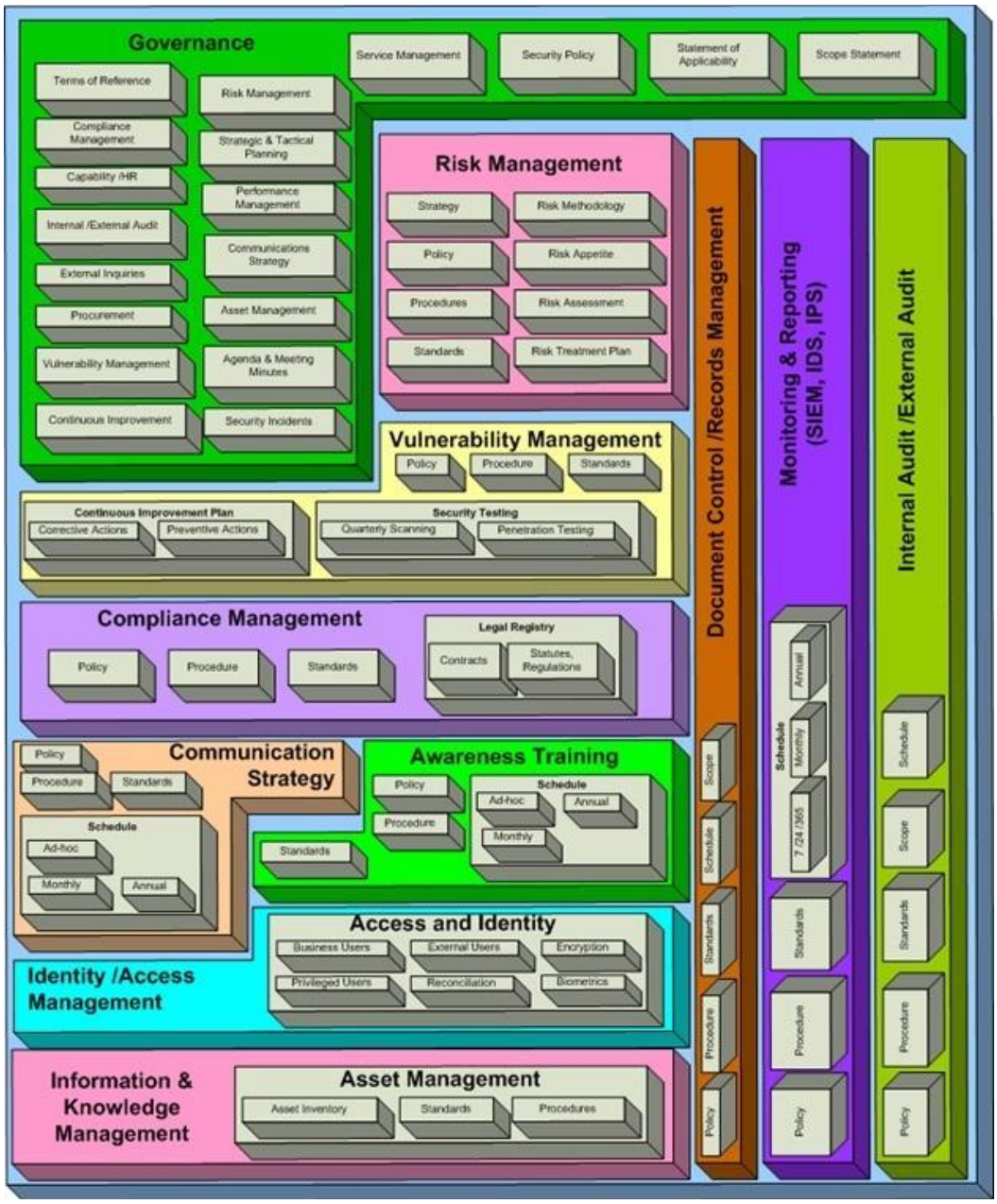


Figure 69: Documentation Content Required to Achieve Full GRC

6.3.9 The researcher adapted and implemented the GRC conceptual, strategic, organisational, technical and cultural aspects identified by Gericke *et al.* (2009, p.10) realising the first instance of the i3GRC™ framework in the private sector case study [CS2]. These have been adapted Table 17 below, in particular noting the scope of the operational requirements.

Fragments of a GRC implementation	
Conceptual	• Establish a governance process, identifying oversight and reporting requirements • Establish risk management based on an enterprise architecture • Establish a compliance management process • Establish a corporate wide GRC repository • Introduce risk and regulatory intelligence
Strategic	• Assure support of top management • Develop a GRC Strategy • Identify required metrics and measurement • Identify roles and responsibilities • Review Cyber Risk Insurance options
Organisational	• Integrate the GRC solution into the planning processes • Integrate the GRC solution into the budgeting processes • Integrate the GRC solution into the reporting processes • Integrate the GRC solution into the investor relations processes • Adapt the business processes from which the GRC key figures are identified • Identify third parties, contracts, relationships, service level agreements, third party management – ensuring adequate provisions for security and privacy • Integrate organisational units and roles
Operational	• Identify system, data and information assets • Conduct Business Impact Assessments (BIA) • Conduct Data Privacy Impact Assessments (DPIA) • Conduct privacy assessments • Conduct security assessments • Conduct risk assessments • If appropriate, conduct FMEA – Failure Mode and Effects Analysis • Identify controls (safeguards) to reduce identified risks –responsive and mitigating • Produce, maintain and update Risk Registers and Risk Treatment Plans (RTP) • Implement controls • Prepare for Incidents – ensure Data Breach Response is adequate and up to date • Ensure Physical Security is part of the whole system design • Ensure Business Continuity Plans (BCP) are in place, accurate and up to date – based on the BIA results • Ensure Disaster Recovery Plans (DRP) are in place, accurate and up to date • Deliver a suite of supporting policies and procedures against which to both deliver the programme and measure it • Develop Monitoring programme • Develop Audit assessment programme • Develop Compliance assessment programme
Technical	• Prepare the steps necessary to set the GRC software system into operation • Integrate the GRC software system into the IS landscape • Do a final inspection and handover the GRC software system • Ensure system monitoring feeds into GRC Monitoring programme
Cultural	• Establish an expert team • Adapt incentive systems of executives/employees • Develop education and training • Conduct education and training road shows

Table 17: i3GRC™ Framework Elements, Adapted from Gericke *et al.* (2009), p.10

6.3.10 Figure 70 provides a visual of how the layers should be reconsidered in the context of i3GRC™. Technology cannot be allowed to continue to hold greater influence over the most important element – the business imperative.

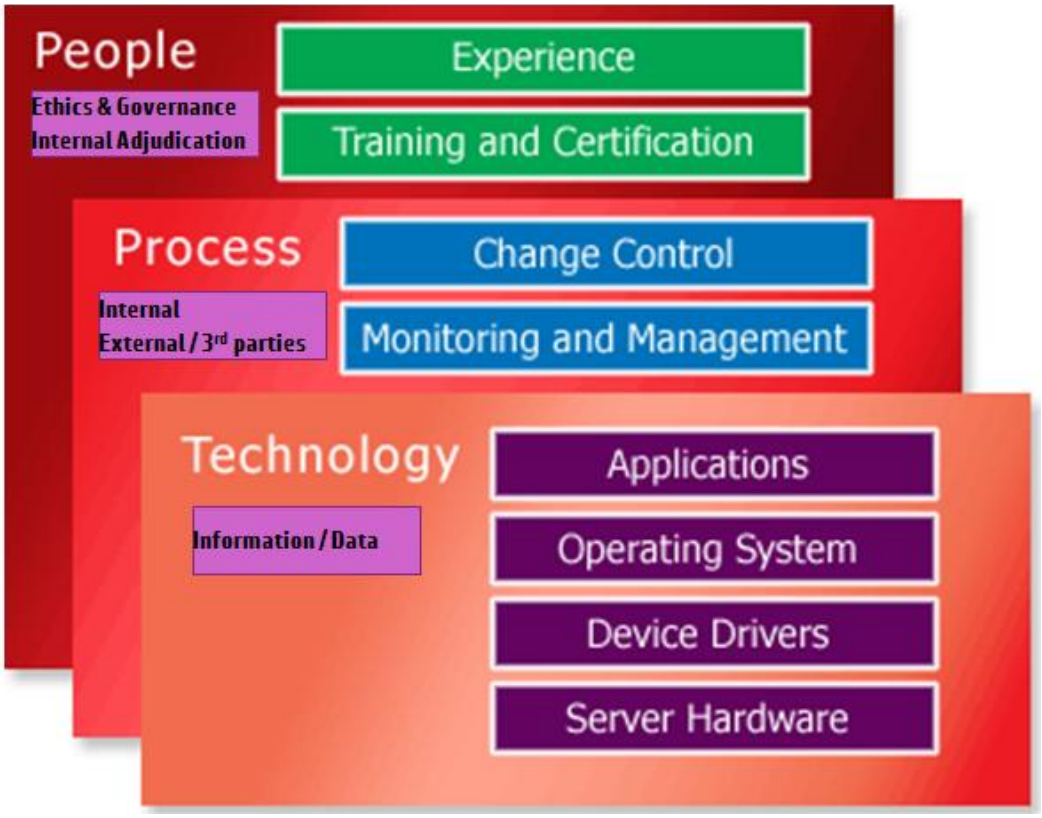


Figure 70: The Availability Equation: PPT, Adapted from Microsoft (2003)

6.3.11 Across the plethora of existing industry Standards, there are obvious core themes running through them. They all have Requirements, many of which are duplicative when reduced to their constituent parts – have a security policy, run antivirus, patch systems, run vulnerability assessments. An organisation need only do these activities once in order to provide the evidence required to show both compliance but also actual embedded IA in action.

6.3.12 The most effective way to measure any improvement programme is through a capability maturity model premise. The maturity model applicable to i3GRC™ is shown in Figure 71 below.

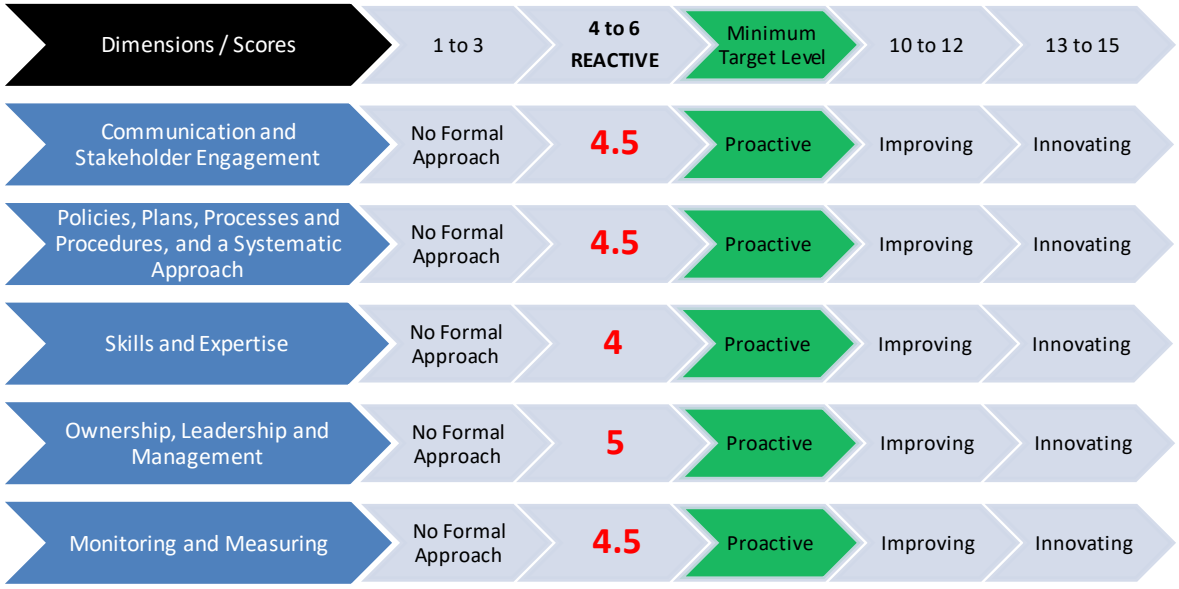


Figure 71: Maturity Model for i3GRC™

6.3.13 This is an adaptation of a BSI STAR model. The expectation is to transition from reactive to proactive – from Level 1, Initial grading through Level 2, Managed (Reactive), through Level 3 (Defined) – which should be the Minimum target level, through to Level 4 (Quantitatively Managed) to Optimizing at Level 5.

6.3.14 For the evaluation of the i3GRC™, the "The Inputs-Outputs-Outcomes-Impacts" model has been adopted through the lens of organisational performance management. The following scope applies to the feedback steps: i) **Input** - people, money, equipment, policies etc; ii) **Activities** - processes – training, logistics, management; iii) **Output** - services provided; services use knowledge; monitoring of what has been invested, done and produced; identifying how *activities* have supported partners achieving their objectives; iv)

Outcome - behaviour; secure practices – say, for example, using a gold disk to ensure consistency of server build; multiple data points providing evidence available for *evaluation* and review; and v) **Impact** - reduced risk[s]; no audit findings; retained customers as a result of satisfactory service received and no breaches experience).

6.3.15 The Owl graphic depicted in Figure 72 provides a visualisation of this evaluation model, derived from the Kellogg Foundation Logic Model.

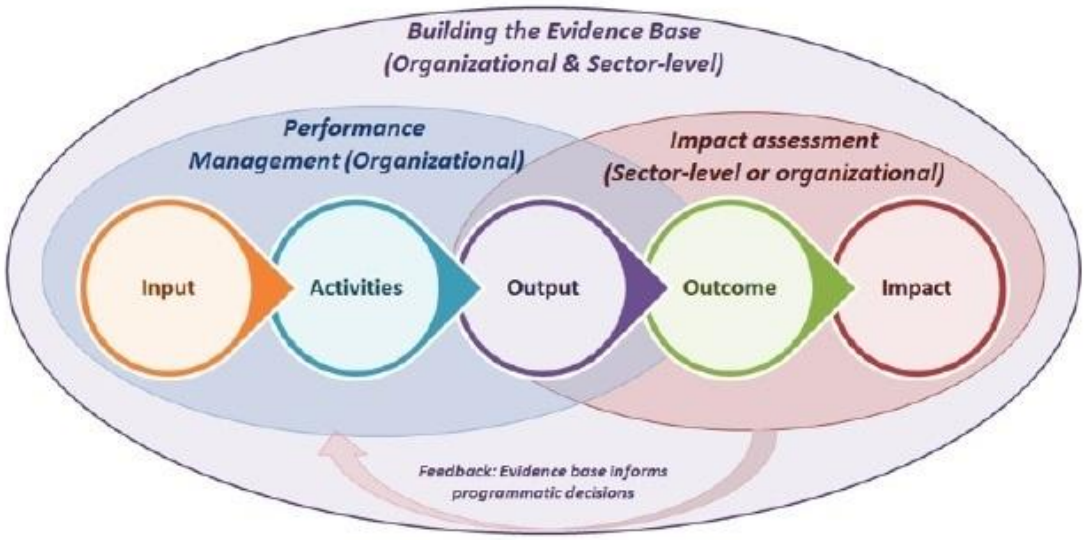


Figure 72: i3GRC™ Evaluation Model, Source: Kellogg (2004)

6.4 Framework Testing and Evaluation

6.4.1 In the private sector case study, i3GRC™ has been used as a mechanism to describe the required integration and education across multiple disciplines in order to move towards a more successful era of IP. An end to end technical description is available in **Appendix II, Section 10.3**. It is also in the early stages of being used in several small to medium enterprises in the UK.

6.4.2 Considering the identified level of complexity in an outsourced service provision environment, consulting is always involved to aid client understanding. However, clarity is not helped if the terminology remains obscure. Figure 73 below provides an example of the resultant corporate bloat and cost to businesses in both the public and private sectors.

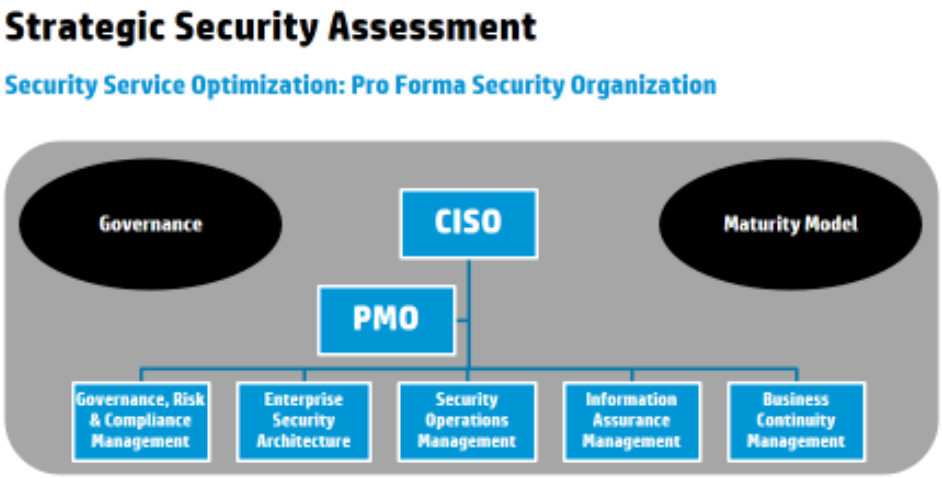


Figure 73: Duplicative Consulting Language, Source: CS2

6.4.3 What is being proposed above is a team structure that requires oversight from a CISO, supported by a Project or Programme Management Officer (PMO), then supported by five separate teams addressing areas that are not individual verticals, all of which have cross-cutting themes. To separate out the work in this manner creates a level of duplication and redundancy that is costly and unacceptable.

6.4.4 Integration is the measurement of GRC maturity. A UCF is required in order to achieve the beating HEART, as described in the Private Sector Case Study [**CS2**]. This requires a level of intelligence and abstract understanding of what each of the governance frameworks – the required legislation, regulation, industry standards and contractual

obligations - are seeking to achieve. This is represented in the pictorial at Figure 74 below, which is by no means comprehensive.

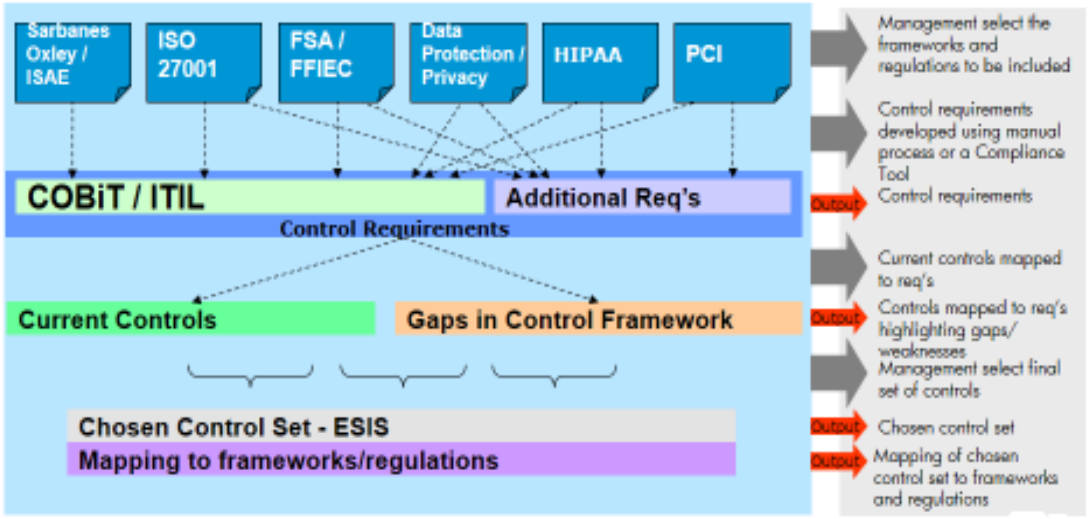


Figure 74: UCF Span

6.4.5 GRC industry technology exists and the researcher has actively engaged in enhancements to one of these toolsets, as part of the theory development of i3GRC™. The development work has seen the incorporation of the research theory building into the practical implementation of an IS that co-ordinates multiple organisational sensors and distils the available data into management level risk reporting. This work is discussed in detail in **Appendix II, HEART** - a Technical Research Conference briefing paper. There are many proponents of management theory (McGregor, Adair, Covey, Drucker, Peters *et al.*) and the InfoSoc appears to be moving the dynamics from Theory X to Theory Y (MIT Sloan, 2011).

6.4.6 The work of Adair, developed in 1973, remains apposite. The Adair model addresses: i) Task completion (what is needed to achieve the mission); ii) Creating and sustaining a group of people to complete the job (building a sustainable team) and Nourish people within the team

(develop individuals). Action centred leadership is required, where three overlapping circles of activity are in balance (Power, 2011, pp.16-17), as depicted in Figure 75 below.

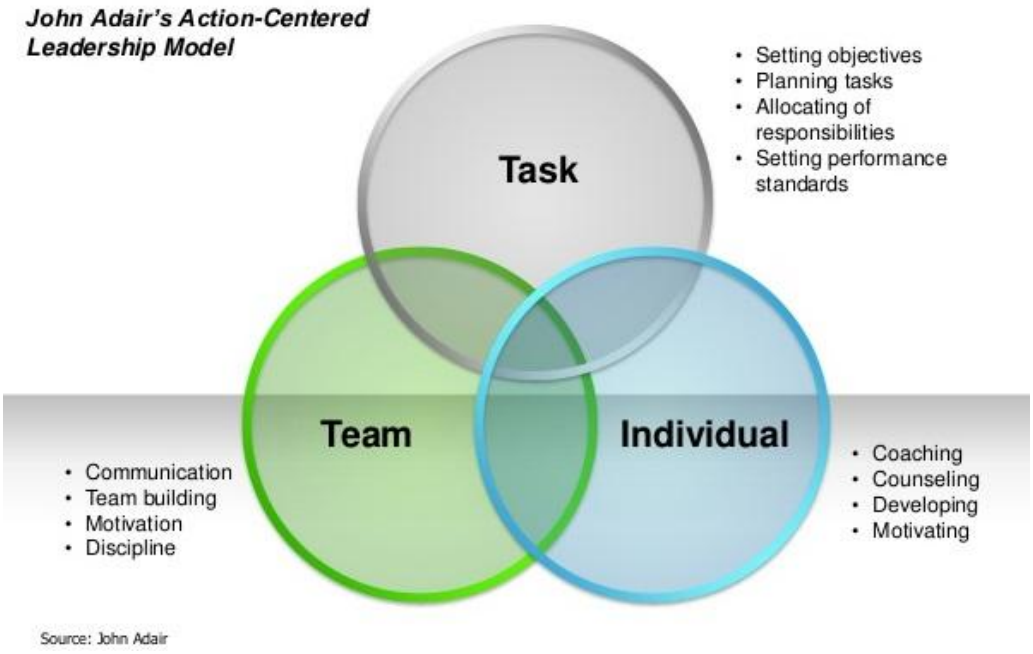


Figure 75: Action-Centered Leadership Model, Source: John Adair cited in Power (2011, pp.16-17)

6.4.7 This is the model the researcher employed as underpinning i3GRC™ in **CS2**. These elements were in balance within the i3GRC™ framework of operation and created an enviable employee work environment. Early indications of application of the framework in commercial settings, in both the private sector global outsourcing organisation represented in the Case Study work (substantive evidence) and other small to medium enterprises (SMEs) (learned observations), is that it is proving workable and appropriate, providing focus and resonance for management reporting; alongside increased effectiveness in internal and external compliance evidence and audit reporting.

6.5 Conclusions

6.5.1 A relatively simple solution is required to this complex and wicked problem. Standard engineering and metadata modelling tools are available and remain relevant. However, IG structures need to have methods of responding to organisational change and disruption, given how prevalent these are in the information age.

6.5.2 The i3 elements remain the challenge – to have achieved successful communication and integration across the multiple information system requirements. To inform, companywide, requires a communications strategy of sufficient depth and commitment to maintain interest and content and distribute this consistently to ensure that the dialogue is two-way thus enhancing reporting. The importance of communication – its creation and delivery – has been a fundamental cornerstone of the IA work carried out by the researcher throughout her career. Strategies for formulating effective communication approaches were written up in one of the books published by the researcher (Simmons, 2012a).

6.5.3 The more effort that is applied to simplification of implementation, the greater the benefits, rather than creating vertical silos for every new trend that arises within the industry. This is part of the discipline integration called for within this research study. This requires strong leadership, something that is not always present. Without leadership empowerment, governance cannot be effectively provided. The theory behind this provides a lodestone to return to regularly. Maintaining clarity on the meanings of the terminology used is also critical.

6.5.4 Table 18 below combines the gaps and barriers identified in Chapter 4 and shows how utilisation of the i3GRC™ framework will facilitate the development of the IA profession, using the theories of professionalisation, when aligned with the existing CBK and skills frameworks, and when understood in the context of intentions to charter the profession.

Finding, gap, barrier	How i3GRC™ speaks to this
IA practitioners do not understand the ontology of InfoSec nor that of IA	Ensuring that understanding starts from an information-centric position will reduce the focus on either InfoSec or IA, placing it squarely on IP in the context of IG. This was identified as necessary in both Case Studies, through observation of phenomena and also through analysis of survey respondents and data analysis.
The shift in dominant narrative from IA to *cybersecurity* creates a schism that could have unforeseen consequences, diluting and narrowing practitioner and policy-maker understanding	Operating with an understanding of the scope of the new framework has been designed to improve the skills of IA practitioners in the context of required organisational outcomes, expanding existing knowledge to incorporate IG.
Self-taught practitioners devalue the long term success of professionalizing IA	Understanding IA in the context of a continuum through to IG will improve the depth of capabilities for IA professionals, as tested through the utilisation of the framework in the private sector case study.
Lack of IA understanding results in higher cost(s) in the short term due to over-reliance on suppliers and technology products selected to reduce risk	Utilisation of a framework that actively encourages participation by all parts of the organisation and removes the IT centric focus is designed to reduce spend and duplication of effort whilst at the same time achieving improved IP and enhanced evidence of information related legislative, regulatory and standards compliance.
IA practitioners do not understand the relationships between InfoSec, IA, and IG	The ontology of IG, once clearly understood by IA practitioners, signifies the progression for IA, to IG, answering the third research question: Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec through to IA? i3GRC™ has been designed to actively encourage this realisation and delivery, through knowledge expansion and thus improving the professional understanding of IA practitioners.

Table 18: How i3GRC™ supports IA Professionalism

6.5.5 In order to ensure the efficiency of the programme, IA practitioners must understand their relationship to other assurance functions and regularly liaise with, rather than compete with, each other, as is often the case in large organisations where power and politics override safety and security (ITGI, 2012, p.31). Data aggregation is also vital – particularly within the context of Big Data, in order to ensure value. Data fusion leads to information superiority and without embedding IA, this is not possible. **[10FS]**

6.5.6 The integration of multiple organisational disciplines is vital to the successful operation of the framework. For example, as identified in the findings (4.11.20) the IA community needs stronger allegiance with Data Scientists in order to understand the data available, "data mining" it appropriately and harnessing the available intelligence contained therein, as depicted in Figure 76.

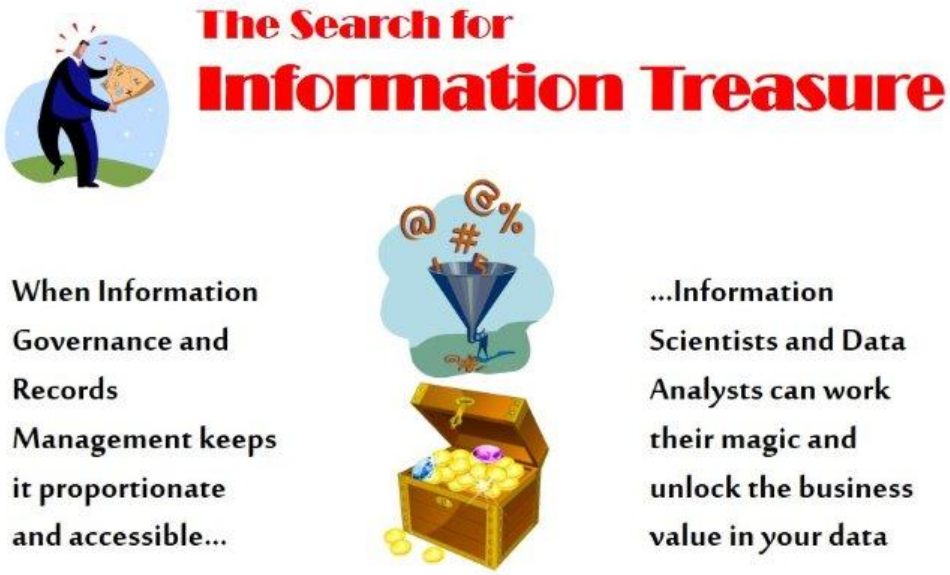


Figure 76: The Search for Information Treasure, Source: Leming (2015)

6.5.7 As a reframing of the Protect, Detect, Respond model, there are three core elements to consider as part of the future strategy for the future of IA: i) RESPECT - people, personalities, politics, professionalism and psychology; ii) REFLECT - best practice, available resources – internal and external; and iii) PROTECT - information, the citizen, connected devices and Society as a whole.

6.5.8 It is intended that organisational utilisation of the i3GRC™ model will help to stop the long, slow drift into failure as identified by Dekker (2011), embedding IA and ensuring its alignment alongside Corporate Governance within the IG spectrum. Process and risk definitions are currently different for Internal Audit, Corporate Risk, Compliance and IT departments. It requires tenacity of purpose in order to achieve the required governance at a content level, to agree on consistency, as well as at an organisational and responsibility level.

7 CONCLUSIONS AND FUTURE WORK

7.1 Conclusions

> "*The future is a refuge from the fierce competition of our forefathers….And the upshot of this modern attitude is really this: that men invent new ideals because they dare not attempt old ideals. They look forward with enthusiasm, because they are afraid to look back*." (Chesterton, 1910)

7.1.1 This chapter summarises the achievements of the research; discusses the limitations that were faced during the study; and identifies the areas of research that require future development.

7.1.2 At the outset of the study, the researcher was a full-time IG and IA consultant, for whom the majority of work had been undertaken in support of UK public sector IA and compliance related activities. The researcher was conscious of a context in which the 21st century experience was one of continued and escalating data breaches, losses and impacts on the InfoSoc that put both individuals and nation states at risk of real harm as a result of poor implementation of the known best practices in IA.

7.1.3 What was evident to the researcher was that gaps in IA practitioner understanding would hinder realisation of the vision and objectives of the United Kingdom (UK) Cyber Security Strategy (previously the UK IA Strategy) to "professionalise IA". Alongside this, the researcher was observing changing use of speech acts with the dominant narrative shifting from IA to cybersecurity. The previous shift had been from InfoSec to IA.

7.1.4 Lack of consensus of norms, with individuals identifying to multiple inter-related groups was exacerbated by a lack of homogeneity of values and viewpoints. The researcher was therefore keen to test IA understanding through challenging the status quo and to further explore IA professionalism and the barriers to achieving the culture change required in order to embed IA as a "business as usual" activity.

7.1.5 The overall research conclusion is that the IA profession is built on a weak foundation due to the lack of collective terminology understanding. The prevailing IA discourse was built on the assumption (in the literature) that "the business" was aware of the available material and cognisant of the significance of elements described therein. However, the research findings showed discrepancies with this assumption on the basis that the core principles of IA, as distinct from InfoSec, have not been widely understood across multiple disciplines, nor embedded for long enough as to be second nature to those who find themselves responsible for the protection of both critical information assets and infrastructure. Stronger professional identity could ensure less risk of loss of IA to cyber.

7.1.6 Creating new models and definitions for the practitioner space must be done carefully, in the context of many existing examples. The researcher believes that the motivations of those involved in IA study should be to ensure they have adequately researched the issues related to the business or industry sector within which they are studying, given that IA is not implemented in the abstract. IA

practitioners should take advantage of the extensive existing BoK rather than duplicating it. The results of these efforts should be the delivery of the required outcomes for effective IP, thus reduced breach levels reaching the news media on a regular basis, and increased trust and confidence in the ability of many to provide adequate IP.

7.1.7 The information infrastructures upon which the InfoSoc is being built are known to be neither safe nor secure enough to act as a trusted basis for the digital society. This research illustrates that enough progress has not been made to secure cyberspace, at a time when growing systemic threats and vulnerabilities have been threatening to undermine confidence in the security of the InfoSoc. At the same time, the cyber threat is growing to a point where the risk is no longer tolerable. This poses risks of broader societal disruption when there is increasing dependence on those same IS.

7.1.8 Market forces alone have not ensured a sufficient level of trust and confidence in information networks. UK Government continues to create new groups to address the challenge, without empowering local police to adequately tackle cybercrime. Public policy needs to lead and shape the IA environment to ensure the InfoSoc was built on robust, resilient and secure foundations whilst business freedoms and civil liberties were protected (IAAC, 2002). The lack of government mandate for standards has not resulted in the market place self-levelling. It is anticipated that the EU GDPR will result in data processing changes across Europe which will have a consequent effect on global businesses. In the researcher's opinion, the EU

GDPR is unlikely to be the panacea some enthusiasts believe it to be, given the narrow area it seeks to address. Much of EU business is reliant on global service provision for which EU law is not the starting point. However, combined with the Network Information Security (NIS) Directive there may be some positive impact on organisational adoption of the change agenda required to embed IA for the sake of appropriate IP.

7.1.9 The concerns raised in this thesis are strategic and operational, national and organisational. It is crucial for IA understanding to have context and scope, to be able to map to client and customer business attributes, technology and tools.

7.1.10 The historical analysis also showed that the challenges have long since been identified and written about, both academically and in the practitioner field. However, the research evidence showed that a great many practitioners are wholly unaware of this history. The lack of understanding is deepening and widening with the passage of time.

7.1.11 It was therefore identified that an important aspect of the research was to review how best to join up the professionalism agenda and apply findings to the continual delivery and improvement of IA within the UK public sector and beyond – in keeping with the Governments' post - Poynter review requirements (Poynter, 2008). The professional membership bodies need to consolidate to reduce the level of overlap and duplication, to be taken seriously and to mature the profession for future decades.

7.1.12 The requirement to *implement* controls in order to deliver IA is often at odds with business requirements for profit margin maintenance and market share increase. As a result, IA practitioners have faced ethical challenges that were not being addressed by the IA professionalism agenda.

7.1.13 In the researcher's experience, excessive use (and regular misunderstanding) of acronyms presents a challenge. This is something the IT industry, in particular, suffers from. Living in an information rich and intelligence poor age is presenting challenges. With the level of confusing and loose terminology coming from the government, it is apparent that the skills crisis will not be solved until the ignorance crisis is solved. What is in existence is an education and, more realistically, an understanding crisis rather than a skills crisis. Education is vital to addressing the skills crisis *but* this must be broad education, with deep learning and broad thinking.

7.1.14 Philosophical thinking and outcomes will help to raise the bar of IA understanding for the professionals involved. Higher education institutions need to consider the impact of the approach of rebranding related InfoSec courses as "cyber", given that this is not tackling the breadth of issues identified in this research as requiring attention. Masters level course content is required.

7.1.15 There are many who have taken on a role that has an IA element with insufficient IA understanding or background learning and are thus not providing an appropriate level of service to their organisations.

7.1.16 The research showed evidence of practitioners working with colleagues who “turn off” at the mere mention of security and who refuse to engage as security is seen as an obstacle to project progression.

7.1.17 There are a number of confusing mixtures of the concepts of ITSEC, InfoSec, IA, IG and, latterly, cybersecurity. There are those practitioners who would advocate the consignment of the CIA triad and the Five Pillars into the waste disposal and insist that improved, directed terminology be used. However, the research indicates that the shift in dominant narrative from IA to cybersecurity is creating a backward step, a wrong turn in the lifespan of IP - from IA to “Computer Security”, addressing the security challenges of computers operating in the cyber domain - reducing the effectiveness of the originally intended best, common and good IA practice. The research showed that the millennial generation are hearing only the term *cybersecurity* and existing *InfoSec* professionals and *IA* practitioners are being side-lined.

7.1.18 It was also felt that there was a need to review the impact of politics and culture on the shifting priorities that hamper the success of embedding best practice that should, by now, be inherent in well-performing organisations. The research showed that greater impact was experienced in budgetary terms as austerity continued to reduce spend.

7.1.19 In the interconnected Information Age, there has never been greater access to information nor adoption of technology. This information

rich, time poor society will experience ongoing anthropological impact and consequences of social change that require deep philosophical thinking. This research has shown the volume of vertical structures that exist, none of which are effectively communicating nor show evidence of understanding the overlaps between each domain. What is required in the immediate future is a more horizontal vision, with disruptive teams and emergent properties of social behaviour, with an understanding of systems engineering.

7.1.20 Secure system design and engineering principles are not uniformly applied in order to provide IP. System Design principles would dictate the need to protect the information contained within any system being designed. In the IoT environment, where form follows function, speed to market and demand for market share in the private sector continues to drive down the adherence to required IA principles. Anderson (1972, p.40) identified this challenge long ago in stating "merely saying a system is secure will not alter the fact that unless the security for a system is designed in at its inception, there are no simple measure to later make it secure".

7.1.21 Artificial Intelligence Security (AIS) and the need to provide assurance as to the ethics and security in place when deploying robotics will be another key factor in the coming years. Even though there may be complexity that is introduced by the scale of the IoT, the core principles of data, application, network, systems and hardware security are still applicable.

7.1.22 The core principles of providing assurance remain relevant and are not limited to the IT profession alone or to IA practitioners. What is required in order to fulfil the UK National Cybersecurity Strategy is implementation of the available best practice elements (and adhering to them), cognisant of the broader understanding of the breadth and depth of IA, beyond cyber.

7.1.23 Schneier (2013a) wrote about the relatively perilous state of the internet (with interconnected platforms whose level of assurance cannot be guaranteed) and the need to be involved in shaping a stronger future. However, the US OPM breach, exposing the PII of over 18 million individuals, which started in 2014, was an example of the worst that can happen as a result of not embedding IA best practice. The fallout from the breach has not been fully realised. The breach impacted the security clearance of many InfoSec professionals across the globe that had heretofore been providing government related consulting services. This breach was yet another example of rampant industrialised insecurity, despite continued investment in cybersecurity.

7.1.24 One of the stated aims of informatics is to design systems that deliver "the right information, to the right person in the right place and time, in the right way" (Cohn, 2015). Advocates of IA have constantly been attempting to secure this delivery using the same quoted phrase and yet there is no evidence of them being aligned with informatics professionals. Across the InfoSec and IA industry, informatics is

neither a term nor a scientific approach that has featured largely in any of the reviewed literature.

7.1.25 The researcher would contend that the conclusions of this research present a reality where IA needs to combine with another complex system - IG – or it will fall by the wayside altogether, wrongly subsumed under the dominant narrative of cybersecurity. The researcher contends that it is in this context that the expectations of the digital economy demand that the IA industry understands and embraces the ontology of IG in order to address the skills crisis faced. This required an expansion of the existing IA professional practitioner identity, knowledge and understanding, through the creation of a new meta framework: Integrated and Informed Information Governance, Risk, and Compliance - i3GRC™.

7.1.26 As the Information Age enters its next phase, focussed on robotics, artificial intelligence, and the IoT, the broader spectrum of informatics and cybernetics need to be more aligned. The adoption of Cyber Assurance would have been a better term along the IP continuum, although it becomes axiomatic. Cyber comes from the Greek word for "governance" so the present shift in dominant narrative from IA to cybersecurity, could have been "governance security".

7.1.27 Whilst the governance of security is absolutely the aim, linguistically and practically speaking, the effective implementation of IA is required in order to appropriately secure cyber space. IA is the objective goal of InfoSec activities; this *includes* cybersecurity. IA is about *assurance* that everything has been done to achieve a risk posture

that suits the needs of the organisation. As a system, IA has become more complex, particularly with the increasing reference to cybersecurity and globalisation and, in order to gain stability, more structure is required. IA is what is achieved when good IG is in place. The researcher believes that the timing of i3GRC™ is apposite.

7.1.28 Guarino (1995) identified that a philosophical and linguistic approach was required and necessary for development of knowledge research. Hypnosis and linguistics are important aspects of the future of social engineering. The research has been influenced by linguistics and cultural anthropology, appreciating how the use theory of meaning and the divergent locutionary aspects of IA and InfoSec interchangeability make a difference to the IA practitioner's ability to implement what is required of them, based on their own sphere of understanding. This can be summed up as having addressed the haecceity (thisness) and quiddity (whatness, essence) of IA - what makes it what it is, including the origins of its definition, beyond that of InfoSec. These are ancient terms grounded in ontological research and address the etymology of the subject area (Aquinas, 1268; Norris, 2015, p.27).

7.1.29 The research sought to test the level of IA understanding as a key aspect of addressing the skills crisis. This research identified an observed need to implement a unified approach to Information Governance (IG) on a large organisation-wide scale, as a result of evolutionary work analysing survey respondents, supported by experience gained over time from engaged PAR involvement in the field being studied (Wadsworth, 1998).

7.1.30 The Grounded Theory premise was that if IA practitioners lack awareness of the fundamental principles of their area of responsibility, it will be impossible to close the gap identified through various studies and surveys and being addressed through the professionalism agenda spearheaded by the UK GCHQ/CESG.

7.1.31 There is a link between this and "the half-life of a fact" – everything we know has an expiration date (Arbesman, 2013) – and this is never more evident than in the InfoSoc, in the information age, dealing with IS.

7.2 Achievements of the Research

7.2.1 This research forms a bridge between theoretical and practical application providing an articulate contribution to IA knowledge and practice, using the acquired knowledge to share and induct know-how into IA professionals (Fitzgerald, 2003). It has achieved the aims and objectives specified in Chapter 1. Specifically, this research has: i) advanced professional IA practice, shortening the identified gaps in IA understanding through practitioner led knowledge sharing; ii) evidenced that there is an extensive body of available material through the literature review and IA Chronology, much of which appears to be unknown to many who proclaim to be "security professionals" which does a great disservice to the success of the IA professionalism agenda; iii) evidenced that the next stage on the IP roadmap is IG, within the maturity from InfoSec to IA to IG (see Figure 1, Figure 24); and iv) provided a unique, new framework to provide organisations

with a holistic roadmap to achieving IP through the implementation of i3GRC™ – integrated and informed information governance, risk and compliance.

7.2.2 i3GRC™ is an instance of an ontology for addressing IA from an enterprise perspective and is the resulting mechanism of this PAR study to visualise and conceptualise the next steps required in the industry to improve practical IP. i3GRC™ can be viewed as a framework within which to articulate an IP conversation. It is not a framework for professionalism nor professionalisation. IA and IG are the outcome of the achievement of *IP*. IA must be achieved in order to be able to evidence IP. The achievement is guaranteed through IG.

7.2.3 The historical chronology is a secondary unique contribution. The historical research method allowed for the review of core texts, highlighting key reports, reviewing them critically, reflecting on their historical impact, political, cultural, economic, geographic and other contexts which made sense of them. This is presented through the lens of holistic organisational IG, rather than through the lens of InfoSec, using content analysis and educated guesses about how audiences interpreted multiple historical texts. This research contributes scientifically to the IS knowledge base of the IA domain, joining it into that of IG and GRC more fully.

7.2.4 A further aim was to identify that, beyond the hard barriers of funding and technology, there are soft barriers in the areas of people, process, and politics that are adding to the lack of understanding of the core concepts required to achieve IP. In **CS2**, the researcher tested and

validated these corporate political aspects, including the need to enhance the OSI model to include more relevant top layers. Ongoing implementation of i3GRC™ continues to prove how valuable this approach is, producing management level reporting not previously visible to the organisation.

7.3 Limitations of the Research

7.3.1 Longitudinal research in the Information Age suffers a time lapse disadvantage that risks the resultant findings being deemed out of date, worse still, irrelevant to the practitioner circles to which they pertain. Alongside this limitation, practitioner research can be prone to over usage of colloquial dialogue, rhetoric, acronyms, and interpretations, which require academic translation.

7.3.2 Another limitation has been the amount and sensitivity of participants, the majority being practitioners in relevant fields. The findings and the description of their circumstances has made it difficult to write them up in full without creating greater vulnerabilities for the represented individuals and organisations concerned.

7.3.3 At each point in the research process, the researcher faced criticism that the subject area was prone to ultracrepidate (Norris, 2015, p.37). The researcher believes this has been necessary to achieve the best outcomes for the research and the future of the IA profession.

7.4 Reflections

7.4.1 If this research had been undertaken in 2015, rather than 2010, it is likely that there would have been greater reference to “cyber”. *Cyber*

is the medium – it is neither the skillset, nor the tool, nor the technology, per se. Digital sabotage is what has been happening, most of the time, *not* "cyber war". However, in May 2017, a new exercise was launched by the UK government to create a comprehensive "Cyber Security Body of Knowledge" (CyBok), to inform and underpin education and professional training for the cyber security sector. Given all the BOK identified through this research it is difficult to estimate the value of this exercise. It is clear from the prevailing rhetoric: the elimination of IA is almost complete. This was a core concern at the start of the research and there is no evidence of the usage of cyber as the dominant narrative succeeding in improving the level of information protection.

7.4.2 The research framework has been systematic but simple. The focus has been on data collection and iterative analysis of the themes that emerged. This research has been valuable in terms of generating a significant volume of relevant historical data regarding IA definitions and maturation. The body of observed data collected during this research, and the systematic analysis that took place, enabled robust conclusions to be generated. The Literature Review presented in *Chapter 2* is extensive. It could be argued that a more focused, narrow literature search would have made the academic location of this work more explicit. The research carried out by Cherdantseva and Hilton (2013b) identified the observable body of work available relating to defining InfoSec compared to IA. Their study and this one

have taken place entirely independently and yet in all likelihood crossed over in terms of timeline and original points of interest.

7.4.3 This research has involved a constellation of ideas, influenced by a number of theoretical positions, in order to situate the work in the areas of professionalism and the information society, providing a dialectical relationship with old knowledge sufficient to create new knowledge as a result. The research addressed questions which are reprised in Table 19 below:

Q#	Question	Methods Utilised	Results
1	*Can IA professional practice be improved through enhanced IA understanding?*	Historical Research, Survey and Interviews, Contextual and Discourse Analysis	This formed the basis of the ontological question, substantiating the reality identified through the research rather than the perceptions of those who have blurred definitions over time. Through critical research, the lack of IA understanding has been empirically evidenced.
2	*How has the extensive body of knowledge influenced professionals?*	Survey and Interviews, Contextual and Discourse Analysis	Discussed in detail in the Findings, Chapter 4. Ill-informed, ill-educated practitioners relying on the inconsistent interpretation of security terminology and resultant requirements are at the heart of the issue of ongoing breaches. The interlocking themes have been articulated as a narrative throughout this research.
3	*Is there a next area of focus for security professionals within the roadmap progression from IT Security, through InfoSec through to IA?*	Contextual and Discourse Analysis, PAR/Case Study	Chapter 5 offers an alternative understanding of conceptual foundations and managerial frameworks of IA. Through the PAR case studies, practitioner research was shown to be able to embed the research within practice in ways that academic research cannot.
4	*Is it possible to produce a framework suitable to support the route from IA to IG?*	Grounded Theory, PAR/Case Study	The research identified the need for a new framework to address the findings, i3GRC™, extrapolated in *Chapters 5* and *6*. Implementing an *Integrated and Informed IG, Risk and Compliance*™ framework across any organisation in any sector will realise IA and provide end-to-end IP. This framework provides a roadmap for a future of mature IG. The framework was in the process of being implemented in CS2, though the researcher's influence on the implementation was cut short as a result of corporate change.

Table 19: Research Questions Results Revisited

7.4.4 This practitioner research highlighted interdisciplinarity throughout, as well as through the theory building, identifying the cross disciplinary requirements for future success. IA is multi-faceted and is not just "down to IT", nor is it "down to Security". Security is ultimately the responsibility of everyone and, as such, IA should be embedded into the roles and responsibilities of everyone. Legal, data, audit, compliance, IG, InfoSec and IT teams need to unify throughout organisations in order to achieve a comprehensive view of their information and extract value from the interactions. In order to grow, it is necessary to ensure wider thinking and action have been encouraged.

7.4.5 The fulcrum of this research has been the UK Cyber Security Strategy (op.cit.). The findings support the theory that tackling the ability to ensure any single country provides a secure environment within which to operate in a complex, chaotic, real world connected setting requires a holistic and systematic approach, through the implementation of the i3GRC™ framework.

7.4.6 The 1980s saw the rise of computing in the workplace and the necessary IP considerations have already been undertaken, the research has been done (Moreton and Chester, 1997, p.59). However, to date, there remains a lack of tangible evidence of successful implementation of embedded security, safety, and protection of information assets. This thesis has evidenced that other priorities have prevailed.

7.4.7 New regulations continue to be developed, along with greater demands for transparency; accurate information about company operations; robust and comprehensive risk management; evidence of regulatory compliance and efficient governance. Changes in IG practices will also be required. Ethical custodianship of data will need to be established in the IoT environment where more data is required to be shared in order to achieve expected efficiencies.

7.4.8 Delivering IA means working within a complex adaptive system (CAS) for which both 100 per cent security and 100 per cent risk-free are unachievable goals (Hercock, 2009). Therefore, the provision of complete assurance is bound by a depth of understanding of the scope of the system(s) and their intricacies. The transfer of risk through the reliance on insurance is an option in the private sector but is not similarly available to the public sector.

7.4.9 The researcher is affected by a society that continues to produce multiple publications on a subject area and yet has less and less well-informed individuals in the roles where the information would be of most value. The overriding impression at the end of the research is that enough has been written, particularly the entreaty that the IA sector must communicate with others, engage in outreach, be mindful of culture (Desman, 2002). Post-structuralism, identifying causes of incidents, errors or breaches is more complex.

7.4.10 Repetition creates legitimacy and normalizes the deviant (Dekker, 2011, p.198). Accuracy is a Newtonian-Cartesian idea and suggests that we can create one definitive account of events based on certainty

and methodological precision. However, the Sony and Ashley Madison breaches indicated that whilst the immediate judgement is usually “cyber-attack”, the reality has turned out to be an “inside job”, usually a disgruntled employee – something that the industry has long been warned to watch out for (Dekker, 2011, p.199).

7.4.11 In a complex system, there is no objective way to determine whose view is right and whose view is wrong (Dekker, 2011, p.200). The requirements for Breach Identification and Incident Management struggle with this dilemma - reparation after an event on the one hand and protection from attack in advance on the other hand. Ultimately, this is nothing new. The castle walls and moat have always required defence.

7.5 Suggestions and Future Work

7.5.1 In this section, suggestions are made as to what future work should be carried out. The nature of the ontological discussions possible in the future is to be welcomed. Depending on the starting point of the researcher, and the direction taken, the benefit of the triangulation of cross referring resources helps to produce a more robust outcome.

7.5.2 This research has opened up the following avenues of research for others to pursue: i) continued incremental enhancement of the i3GRC™ framework to allow the conversion of the framework to a fully mature roadmap that would effectively address the requirements of organisations to embed IP, as well as syntax development to support the graphical representation; ii) development of a competency framework to overlay IG on the IA competency framework, and align

with the Valentine (2015) competency framework research carried out to achieve Enterprise Technology Governance; iii) research into the confusion and misunderstanding(s) caused by excessive use of acronyms as shorthand for communication; iv) ensuring improved agenda correlation and membership consolidation focus across the Institute of Directors (IoD), the Chartered Institute of Personnel (CIPD), Chartered Quality Institute (CQI) and the Institute of Internal Auditors (IIA) with regard to embracing IG; v) review of the quality and adjudication of the provision of existing cyber related courses to assess adequacy of scope; vi) analysis of risk versus reward dynamics of business in relation to its impact on IA professionalism; vii) identification of the impact on future security models, where data losses experienced have escalated exponentially and, in parallel, the level of public dismay dims as they become inured; viii) investigation into the connection of professionalisation and ethics to i3GRC™ and ix) analysis of the barriers to adopting a reservation of title and/or reservation of function (Bott, 2005) adaptation to the existing professional membership bodies structure.

7.5.3 The researcher has worked closely with Goodger (2011a/b), throughout the period of this study and intends to continue to do so where the lines of enquiry have converged: the InfoSoc, Big Society, and the IoT. Goodger's work is looking at the integrated Information Ecosystem (aka Cyberspace) on the premise that Understanding, Protecting, Sustaining and Nurturing are the keystone capabilities required to safeguard the UK's. This is addressing *small world*

thinking, providing a Lodestone for future organisational framework development (Goodger, A. and Atkinson, S. R. (2011a/b).

7.5.4 The researcher intends to work directly with David Miller on Active Management and Active Governance, addressing large IT outsourcing arrangements and contract management (Miller and Woodman, 2015).

7.5.5 Finally, the researcher intends to work with leading UK academics to establish links between ISMS and i3GRC™.

Part 4a – References and Bibliography

Due to the scale of the historical review, an extensive Bibliography is listed separately in support of the References provided hereunder which denote the citations found throughout the Thesis content.

8 REFERENCES

Abercrombie, N., Hill, S. and Turner, B. (2000) *The Penguin Dictionary of Sociology.* London: Penguin. p.372

Abdullah, N., Sadiq, S. and Indulska, M. (2011) A Framework for Industry-Relevant Ontology Development. *ACIS 2011 Proceedings.* Paper 80. [online]. [Accessed 16 August 2015]. Available at: http://aisel.aisnet.org/cgi/viewcontent.cgi?article=1079&context=acis2011

ACCA (2010a) Five Minutes On....Risk and Reward: Shared perspectives. *Accountants for Business*. Association of Chartered Certified Accountants.

ACCA (2010b) Risk and reward: tempering the pursuit of profit: executive summary. *Accountants for Business.* [online]. June. [Accessed 12 July 2015]. Available at: http://www.accaglobal.com/content/dam/acca/global/PDF-technical/corporate-governance/tech-afb-rarexec.pdf

ACCA (2010c) Risk and reward: tempering the pursuit of profit: full report, *Accountants for Business.* [online]. [Accessed 12 July 2015]. Available at: http://www.accaglobal.com/content/dam/acca/global/PDF-technical/corporate-governance/tech-afb-rar.pdf

Ackerman, R.K. (2013) The Fidelity of Data, *Signal Magazine,* July. AFCEA.

ACPO (2005) *Code of Practice on the Managing of Police Information* (MOPI) – National Centre for Police Excellence. [online]. Home Office. July 2005. [Accessed 6 March 2011]. Available at: http://www.npia.police.uk/en/15088.htm

AIIM (2014) *It's not IG, It's Information Opportunity: Executive Summary*, www.aiim.org

AIRMIC (2002) *A Risk Management Standard*, AIRMIC, ALARM, IRM, www.airmic.com

AIRMIC, Alarm and IRM (2010), *A structured approach to Enterprise Risk management (ERM) and the requirements of ISO 31000.* [online]. [Accessed 12 July 2010]. Available at: https://www.theirm.org/media/886062/ISO3100_doc.pdf

ALARM (2000) *Corporate Governance in the Public Sector – The Role of Risk Management.* Alarm

Alleyne, R., Gentile, J. Waters, J., Albinger, W. and Maloney, P. (2016) *Legal Assurance in the ERM Framework*, ACC Docket, January 2016 [online]. [Accessed 12 May 2017]. Available at: http://www.accdocket.com/articles/legal-assurance-in-the-erm-framework.cfm

Ampoma, M. (2012) *The Innovative Communicator: Putting the soul back into business.* Indiana: Balboa Press. p.ix

Anderson, D. (2015) *A Question of Trust: Report of the Investigatory Powers Review.* London: OGL. [online]. June. [Accessed 3 December 2015]. Available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

Anderson, J. P. (1972) *Computer Security Technology Planning Study*, ESD-TR-73-51, ESD/AFSC, Hanscom AFB, Bedford, MA ([NTIS AD-758 206]; Volumes **I** and **II**. [online]. [Accessed 4 September 2015]. Available at: http://seclab.cs.ucdavis.edu/projects/history/papers/ande72a.pdf and http://seclab.cs.ucdavis.edu/projects/history/papers/ande72.pdf

Anderson, L. (2009) *Information Landscape*, a presentation prepared for EURIM [DP Alliance] IG Working Groups. [online]. [Accessed 15 March 2016]. Available at: http://www.eurim.org.uk/activities/ig/bp/bp.php

Anderson, R.J. (2001) Why InfoSec is Hard - An Economic Perspective. Paper presented at the *Proceedings 17th Annual Computer Security Applications Conference*. IEEE Computer Society, Los Alamitos, California. [online]. [Accessed 17 January 2011]. Available at: http://www.acsac.org/2001/papers/110.pdf

Anhal, A., Daman, S., O'Brien, K. and Rathmell, A. (2002) *Engaging the Board: Corporate Governance & Information Risk*. IAAC. [online]. [Accessed 15 March 2016]. Available at: https://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1692.pdf

Anhal, A., Gibson, S. and Valeri, L. (2003) *Promoting Information and Network Security awareness Among Citizens: A Global Report and Lessons Learned.* A RAND Report

Aquinas, T. (1268) *Summa Theologiae*, London: Blackfriars, 1964–1976: i, quaest. 84, art. 7: "*quidditas sive natura in materia corporali*"

Arara, A., Fgee, E.B. and Bargelail, M. (2015) Requirements of IA. In *International Conference on Computer Science, Data Mining & Mechanical Eng.*, Bangkok, Thailand. [online]. [Accessed 20 September 2015]. Available at: http://iieng.org/siteadmin/upload/1318E0415040.pdf

Arbesman, S. (2013) *The Half Life of Facts: Why Everything We Know Has An Expiration Date.* 2nd edition. Boston: Penguin

Armstrong, J., Rhys-Jones, M. and Rathmell, A. (2002) *IA & Corporate Governance: What Every Director Must Know.* A RANDEurope collaboration

Ashenden, D. (2007) BCS group aims to spread lessons of IA to the masses, *Computer Weekly*. [online]. [Accessed 25 May 2015]. Available at: http://www.computerweekly.com/news/2240079951/BCS-group-aims-to-spread-lessons-of-information-assurance-to-the-masses

Ashford, W. (2015) *Financial sector data protection breaches up 183% in past two years*, Computer Weekly [online]. 3 June. [Accessed 7 March 2015]. Available at: http://www.computerweekly.com/news/4500247427/Financial-sector-data-protection-breaches-up-183-in-past-two-years

Ashforth, B.E., Harrison, S.H. and Corley, K.G. (2008) Identification in organizations: An examination of four fundamental questions. *Journal of Management*, **34**(3), pp.325-374

Ashley, B., Cox, S., Dean, T. and Stimeare, R. (1999*) IA – the Achilles' Heel of Joint Vision 2010*?. [online]. [Accessed 2 February 2011]. Available at: http://www.iwar.org.uk/rma/resources/airchronicles/ashley.htm

Atlantic Council (2007) *Cyber Attack: Risk Management Primer for CEOs.* [online]. [Accessed 15 March 2016]. Available at: http://www.atlanticcouncil.org/publications/reports/cyber-attack-risk-management-primer-for-ceos

Audit Commission (1994a) *High Risk/High Potential: An Executive Report on the Management of Information Technology in Local Government.* London: Audit Commission

Audit Commission (1994b) *High Risk/High Potential: A Management Handbook on IT in Local Government.* London: Audit Commission

Audit Commission (2001) *Worth the risk: Improving risk management in local government.* [online]. [Accessed 8 February 2011]. Available at: http://www.audit-commission.gov.uk/nationalstudies/localgov/Pages/worththerisk.aspx

Audit Commission (2002) *Councils and e-Government, Research so far*

Audit Commission (2010) *Data Quality Standards.* [online]. [Accessed 8 March 2011]. Available at: http://www.audit-commission.gov.uk/aboutus/howwearerun/ourstrategy/strategicobjectives/dataquality/Pages/Default.aspx

Backhouse, J. with Bener, A., Chauvidul, N., Wamala, F. and Willison, R. (2003) *Social Risk Management – Practices and Behaviour in Cyberspace*, report prepared for the Foresight Cyber Trust and Crime Prevention Project, London

Ballard, M. (2010) HM Courts Service staff breached government database of personal information, Computer Weekly. [online]. [Accessed 11 March 2016]. Available at: http://www.computerweekly.com/news/1280093280/HM-Courts-Service-staff-breached-government-database-of-personal-information

Bannister, F. (2002) The Dimension of Time: Historiography in IS Research. *Electronic Journal of Business Research Methods*. **1**(1)

Barman, S. (2002) *Writing InfoSec Policies.* 2nd edition (1st edition, 2001), p.11. Indiana: New Riders

Barwise, M. (2013) Role with IT, *ITNow Magazine*, BCS, pp.30-31

Baskerville, R. (1999) Investigating IS with Action Research. *Communications of the AIS.* **2**:19

BCS (2003) *BCS campaigns for broader ICT membership*. [online]. [Accessed 27 September 2015]. Available at: *http://www.bcs.org/server.php?show=conWebDoc.1799*

BCS (2010) *IT and the Professionalism Debate*. [online]. [Accessed 27 September 2015]. Available at: http://www.bcs.org/content/conEvent/5383

Beaming (2017) *Cyber Reports.* [Accessed 29 April 2017]. Available at: https://www.beaming.co.uk/support/cyber-reports/

Beauregard , J.E. (2001) *Modelling IA,* MS Thesis, USAF AFIT/GOR/ENS/01M-03, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio. [online]. [Accessed 2 February 2011]. Available at: http://www.iwar.org.uk/iwar/resources/usaf/maxwell/students/2001/afit-gor-ens-01m-03.pdf

Bediako, T. (2014) ERM – Integrated Framework*, ISACA's IT Audit, InfoSec & RISK Insights,* p.30. [online]. [Accessed 15 March 2016]. Available at: http://www.isaca.org/chapters9/Accra/Events/Documents/ERM%20ISACA.pdf

Bell, T.J. (2010) The Social Psychology of IT Security Auditing from the Auditee's Vantage Point: Avoiding Cognitive Dissonance. *ISACA Journal.* Volume **3**

Benbasat, I., Goldstein, D.K. and Mead, M. (1987) The Case Research Strategy in Studies of IS. *MIS Quarterly.* **11**(3), pp.369–386

Benson, Lord (1992) *Criteria for a group to be considered a profession*. As recorded in Hansard (House of Lords). Debate 08. July 1992 Volume 538. cc1198-234

Berkley, W.E. (2012) There is nothing new under the sun, *Ecclesiastes 1:4-11*, [Accessed 14 September 2016]. Available at: http://www.bible.ca/ef/expository-ecclesiastes-1-4-11.htm

Berners-Lee, T. (2009) *Raw Data Now*, TED. [online]. [Accessed 6 February 2011]. Available at: http://www.ted.com/talks/tim_berners_lee_on_the_next_web.html

Best, D. (1996) *The Fourth Resource: Information and Its Management.* Hampshire: Aslib Gower

Birchall, D., Ezingeard, J-N. and McFadzean, E. (2003*) InfoSec: Setting the boardroom agenda*, London: Grist, based on original work entitled "Perception of risk and the strategic impact of existing IT on InfoSec strategy at board level"

Birchall, D., Ezingeard, J. N., McFadzean, E., Howlin, N. and Yoxall, D. (2004) *IA: Strategic alignment and competitive advantage,* London: Grist Ltd

Bishop, M. (2003) *Computer Security, Art and Science*, Boston: Pearson Education, Inc for Addison Wesley

Blair, B.T. (2014) *15 Key Insights from the IGI Annual Report 2014. [*online]. [Accessed 14 March 2016]. Available at: https://www.linkedin.com/pulse/20140820164329-396452-15-key-insights-from-the-igi-annual-report-2014

Blyth, A.J.C. and Kovacich, G.L. (2001) *IA – surviving in the information environment.* London: Springer-Verlag

Blyth, A.J.C. and Kovacich, G.L. (2006) *IA – security in the information environment.* 2nd edition. p. 83. London: Springer-Verlag

Boulding, K.E. (1956) *General Systems Theory – The Skeleton of Science.* Management Science. University of Michigan, pp.197-208. [online]. [Accessed 16 August 2015]. Available at: http://dx.doi.org/10/1287/mnsc.2.3.197

Bott, F. (2005) *Professional issues in information technology*. Swindon: BCS, The Chartered Institute

Boyce, J.G. and Jennings, D.W. (2002) *IA: Managing Organizational IT Security Risks.* London: Butterworth Heinemann

Brock, A. (2006) Dimensions of early years professionalism: Attitudes versus competences. Paper from the *Association for the Professional Development of Early Years Educators (TACTYC).* [Accessed 12 March 2017]. Available at: www.tactyc.org.uk/pdfs/Reflection-brock.pdf

Brewer, R. (2007) *Your PhD Thesis – How to plan, draft, revise and edit your thesis.* Abergele: Studymates Limited

Brin, D. (1998) The Transparent Society, Massachusetts: Basic Books

Burnburg, M.K. (2003) *A Proposed Framework for Business InfoSec based on the concept of Defense-in-Depth*, Springfield, Illinois: University of Illinois

Burton, E. (2008) *Final Report into the loss of MoD Personal Data*. [online]. [Accessed 7 February 2011]. Available at: http://www.mod.uk/nr/rdonlyres/3e756d20-e762-4fc1-bab0-08c68fdc2383/0/burton_review_rpt20080430.pdf

Burton, E. (2011) *How can the science, technology and business management communities play a leading role in shaping an uncertain environment?* Stevenson Science Lecture. Royal Holloway, University of London

Burton, E. (2015) *Closing remarks,* IAAC Annual Symposium – the Citizen and the IoT

Bush, S. and Evans, S. (2001) *IA Design and Assessment - A Fundamental Science-Based Approach to IA*, Final Report for Period March 2000 – August 2001 Contract No. F33615-00-C-1629, GE Corporate Research & Development. [online]. [Accessed 2 February 2011]. Available at: http://www.crd.ge.com/~bushsf/InfoAssurance.pdf

Bush, V. (1988) As we may think. In *Computer-supported cooperative work,* Morgan Kaufmann Publishers Inc., pp.17-34

Busha, C. and Harter, S.P. (1980) *Research Methods in Librarianship: techniques and interpretations*, New York: Academic Press

Business Software Alliance (2002) Government at Risk for Major Cyber Attack in Next 12 Months, *IT Pros Say*. [online]. [Accessed 16 August 2015]. Available at: https://www.entrust.com/news/government-at-risk-for-major-cyber-attack-in-next-12-months-it-pros-say/

Cable, V. (2017) *BCS Apprenticeships*, 8 February 2017, London. [online]. [Accessed 5 May 2017]. Available at: https://www.youtube.com/watch?v=x4bCyFMvAzI

Cadbury, A. (1992) *The Financial Aspects of Corporate Governance*. London: Professional Publishing Ltd. [online]. 1 December [Accessed 6 March 2011]. Available at: http://www.ecgi.org/codes/documents/cadbury.pdf

Calder, A. and Watkins, S. (2008) *IT Governance, A Manager's Guide to Data Security and ISO27001/ISO27002,* 4th edition, London: Kogan Page

Cameron, D. (2015) *My vision for a smarter state*, Prime Minister's Office, Localism speech. [online]. [Accessed 3 October 2015]. Available at: https://www.gov.uk/government/speeches/prime-minister-my-vision-for-a-smarter-state

Caplan, K. and Sanders, J.L. (1999) Building an international security standard. *IT professional*, **1**(2), pp.29-34

Carnegie Mellon (2012) *InfoSec Assurance Capability Maturity Model (ISA-CMM).* Version 3.2. [online]. [Accessed 15 March 2016]. Available at: http://www.isatrp.org/ISA-CMM/ISA-CMMv3_2-DRAFT-20120330.pdf

Cave, B. (2015) *2015 Data Breach Litigation Report: A comprehensive analysis of class action lawsuits involving data security breaches filed in United States District Courts*. [online]. HROBOU\128134.11 [Accessed 11 March 2016]. Available at: http://bryancavedatamatters.com/category/white-papers/white-papers-data-breach/

Cayton, H. (2006) *IG in the Department of Health and the NHS*

Caza, B.B. and Creary, S.J. (2016) *The construction of professional identity* [Electronic version]. [Accessed on 12 March 2017] Available at: http://scholarship.sha.cornell.edu/articles/878

Cebula, J.J. and Young, L.R. (2010) *A Taxonomy of Operational Cyber Security Risks*. [online]. Technical Note. CMU/SEI-2010-TN-028. CERT Program. [Accessed August 2011]. Available at: http://www.sei.cmu.edu

CERT (2010) *Resilience Management Model.* Version 1.0

Checkland, P. (1991) From framework through experience to learning: the essential nature of action research. *IS Research: Contemporary Approaches and Emergent Traditions.* H-E. Nissen, H.K. Klein, R.A. Hirschheim (eds.). North-Holland, Amsterdam. pp.397-403

Cherdantseva, Y. (2014) *Secure*BPMN – a graphical extension for BPMN 2.0 based on a Reference Model of IA & Security.* Thesis. Cardiff University, December

Cherdantseva, Y. and Hilton, J. (2013a) InfoSec and IA: Discussion about the Meaning, *Organizational, Legal, and Technological Dimensions of Information System Administration.* **167**

Cherdantseva, Y. and Hilton, J. (2013b) *Reference Model for IA and Security.* Cardiff University. [online]. [Accessed 2 September 2015]. Available at: https://www.google.co.uk/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0CDIQFjACahUKEwiC3ZTwjdjHAhWBQBQKHdfOCT8&url=http%3A%2F%2Fusers.cs.cf.ac.uk%2FY.V.Cherdantseva%2FRMIAS.pdf&usg=AFQjCNF-PFkc-pBl3joZs2EjZ_jegKumow&sig2=dqvLe5GLGgbeuEyfecVz6g and https://en.wikipedia.org/wiki/Reference_Model_of_Information_Assurance_and_Security and http://rmias.cardiff.ac.uk/ - by Wikilubina - Own work. Licensed under CC BY-SA 3.0 via Commons - https://commons.wikimedia.org/wiki/File:A_Reference_Model_of_Information_Assurance_and_Security_(RMIAS).png#/media/File

Chesterton, G.K. (1910) *What's Wrong with the World,* ISBN**:** 3849677672

Cimtech (2011) *The Future of Electronic Information and Records Management in the Public Sector: Meeting IG Challenges in 2011.* Workshop presentation notes. Hatfield, Fielder Centre: Cimtech with The National Archives

Chissick, M. and Harrington J. (2004*) E-Government A Practical Guide to the Legal Issues.* Field Fisher Waterhouse. London: Thomson Sweet & Maxwell

Chittoor, J. (2014) *e-Governance Competency Framework for Digital India with Implementation Toolkit.* [online]. [Accessed 5 October 2015]. Available at: http://www.academia.edu/10224920/e-Governance_Competency_Framework_for_Digital_India_with_Implementation_Toolkit

CIPFA (2001) *Risk Management in the Public Services*, CIPFA and Alarm. [online]. [Accessed 8 February 2011]. Available at: http://learning.cipfa.org.uk/alc/category/default.asp?content_ref=2098

Clarke, H.E. (2009) *Why is Assurance so important?* [online]. [Accessed 1 September 2015]. Available at: http://www.metrosky.co.uk/docs/Why_is_assurance_so_important.pdf

Clarke, S. (2015) *Scaling Vendor and Project Security Risk – Are you going to assess them all?* Infospectives. [online]. [Accessed 20 April 2015]. Available at: http://infospectives.co.uk/2015/04/14/scaling-vendor-and-project-security-risk-are-you-going-to-assess-them-all/

Cohn, R. (2015) *Informatics (academic field),* Miami: Book on Demand. [online]. [Accessed 18 April 2015]. Available at: http://www.abebooks.com/9785511783956/Informatics-Academic-Field-5511783951/plp

Cole, E. (2002) *Hackers Beware: Defending Your Network from the Wiley Hacker.* US: New Riders Publishing

Coleman, N. (2005a) *Briefing Paper: Professionalisation of the InfoSec industry*

Coleman, N. (2005b) *IA: A review of UK Government and industry initiatives.* Cabinet Office. Chair of the Security Alliance for Internet and New Technologies (SAINT)

Coleman, N. (2007) *Independent Review of IA, Summary and Recommendations*. Cabinet Office / CSIA

Coleman, N. (2008) *Independent Review of IA, The Coleman Report.* Cabinet Office. [online]. [Accessed 15 March 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60967/ia_review.pdf

Coles-Kemp, E. (2008) *The anatomy of an InfoSec management system*, Thesis, King's College London (University of London)

Coles-Kemp, E. (2009a) *The Effect of Organisational Structure and Culture on InfoSec Risk Processes,* Administrative Science Quarterly, **17**(1), 1-25

Coles-Kemp, E. (2009b) *Privacy – Governance Challenges*, Presentation for EST_tcm6-32696

Collins, T. and Bicknell, D. (1997) *Crash: Learning from the world's worst computer disasters*, London: Simon & Schuster Ltd

Commission of the European Communities (2001) *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, Communication from the Commission to the Council, The European Parliament

Commission of the European Communities (2002) *Council Framework Decision on attacks against IS* (presented by the Commission) [online]. Reference C5-0271/02. Brussels. COM(2002) 173 final. 2002/0086 (CNS). [Accessed 14 March 2016]. Available at: http://www.europarl.europa.eu/registre/docs_autres_institutions/commission_europeenne/com/2002/0173/COM_COM(2002)0173_EN.pdf

Condon, R. (2010) *ISF,* (ISC)² *and ISACA have worked together to create 12 principles intended to help business and security teams understand and aid each other*. [online]. [Accessed 6 October 2015]. Available at: http://www.computerweekly.com/news/1525516/ISF-ISC2-and-ISACA-team-up-on-IT-security-principles-guidelines?asrc=EM_USC_13287173&track=NL-1019&ad=812603

Conklin, Wm. A. and McLeod, A. (2009) *Introducing the ITSec EBK Framework*. [online]. [Accessed 7 June 2015]. Available at: www.amcleod.com/mcleod9.pdf

Conrad, F.G. and Schober, M.F. (1999a) Conversational Interviewing and Data Quality. *New School for Social Research. [*online]. [Accessed 15 June 2011]. Available at: http://www.fcsm.gov/99papers/conrad2.pdf

Conrad, F.G. and Schober M.F. (1999b) *A Conversational Approach to Text-Based Computer-Administered Questionnaires, in* Proceedings of the Third ASC International Conference, pp.91–102. Chesham, UK: Association for Survey Computing

Cook, R.I. (2000) *How Complex Systems Fail*, Cognitive Technologies Laboratory, University of Chicago

Cooper, G.L. (2011) *"in my opinion"* – on Management Books, *Management Today*, p.78

Coquillette, D.R. (1993) Professionalism: The deep theory. *NCL Rev.*, **72**, p.1271

Corbin, J. and Strauss, A. (2008) *Basics of Qualitative Research*, 3e, London: Sage Publications

Cordery (2015) *European Court rules Safe Harbor invalid in Schrems case.* [online]. [Accessed 15 March 2016]. Available at: http://www.corderycompliance.com/european-court-rules-safe-harbor-invalid-in-schrems-case/

Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2011) *Cyber Security and the UK's Critical National Infrastructure:* A Chatham House Report. [online]. [Accessed 26 September 2015]. Available at: https://www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/r0911cyber.pdf

COSO (2006) *COSO ERM model of future goal state, Guide to ERM, FAQ*, Protiviti Independent Risk Consulting, ERM FAQ Guide, p.10, PRO-1108-101000

Cox, L. (2010) *Creating a profession and a body of knowledge for product supportability engineering at high-tech companies*. California State University, Dominguez Hills.

Cunningham (2015) Experian shares fall sharply after T-Mobile data breach, *Telegraph Business report*. [online]. [Accessed 4 October 2015]. Available at: http://www.telegraph.co.uk/finance/markets/ftse100/11906233/Experian-shares-fall-sharply-after-T-Mobile-data-breach.html

Curmudgeon (2015) The Five Horsemen, The Curmudgeon. *ISSA Journal.* June. **13**(6), p.39

Czech Republic (2011) *Cyber Security Strategy of the Czech Republic for the 2011-2015 Period. [*online]. [Accessed 22 September 2015]. Available at: http://www.enisa.europa.eu/media/news-items/CZ_Cyber_Security_Strategy_20112015.PDF

D'Aubeterre, F., Singh, R. and Iyer, L. (2008) Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes. *European Journal of IS.* [online]. **17**, pp.528-542, doi:10.1057/ejis.2008.42. [Accessed 31 May 2015]. Available at: http://www.palgrave-journals.com/ejis/journal/v17/n5/full/ejis200842a.html

Daman, S. (2006) *IA in a Global Bank.* Presentation to BCS Birmingham ITSec Conference. HSBC Holdings plc.

Dark, M.J., Ekstrom, J.J. and Lunt, B.M. (2006) Integrating IA and Security into IT Education: A Look at the Model Curriculum and Emerging Practice. *Journal of IT Education*, Volume **5**

Davies, T. (2010) Black swans, turkeys, ostriches and other Christmas poultry. *Risk Management Today.* Todd Davies and Associates. [online]. [Accessed 2 September 2015]. Available at: http://www.todddavies.com.au/_bpost_4851/Black_Swans,_Turkeys,_Ostriches_and_other_Christmas_Poultry_%E2%80%93_a_tale_of_Strategic_Risk

de Silva, R. (2011a) *Government vs. Commerce: The Cyber Security Industry and You (Part One*)

de Silva, R. (2011b) *Protection for Hire: The Cyber Security Industry and You (Part Two)*

Dekker, S. (2011) *Drift Into Failure: From Hunting Broken Components to Understanding Complex Systems.* Ashgate Publishing Ltd

Deloitte University Press (2015) *Ignoring bad news: How behavioural factors influence us to sugarcoat or avoid negative messages*. [online]. [Accessed 22 September 2015]. Available at: http://d2mtr37y39tpbu.cloudfront.net/wp-content/uploads/2015/08/DUP_1214_IgnoringBadNews.pdf

DeMarco, T. and Lister, T. (2013) *Peopleware: Productive Projects and Teams,* 3rd edition, New York: Dorset House Publishing

Denning, D. (2000) *Information Warfare and Security*, 4th edition, New York: Addison Wesley

Desman, M.B. (2002) *Building an InfoSec Awareness Program*, p.xvi, Florida: CRC / Auerbach Publications

Digital Policy Alliance (ongoing), Formerly EURIM, now DPA, various outputs available at: http://dpalliance.org.uk/publications-index/

Dimitriadis, C.K. (2011) InfoSec from a Business Perspective. *ISACA Journal.* [online]. Volume **1**. [Accessed 18 Feb 2011]. Available at: http://www.continuitycentral.com/feature0856.html

Dimopoulos, V.A. (2007) *Effective IA with Risk Management.* PhD Thesis. University of Plymouth

Dowdall, J., Mattinson, H. and Fagan, P. (2011) *2011 Census Security: Report of the Independent Review Team.* ONS. [online]. January. [Accessed 25 May 2015]. Available at: http://www.nisra.gov.uk/archive/census/2011/2011_Census_IIAR.pdf

Dunkel, D. (2010) The New Norm: IA. *Integration Intelligence.* SDM International BNP Media. [online]. March. [Accessed 3 December 2015]. Available at: http://www.sdmmag.com/articles/85383-the-new-norm-information-assurance

Dutton, J.E., Roberts, L.M. and Bednar, J.S. (2010) Pathways for positive identity construction at work: Four types of positive identity and the building of social resources. *Academy of Management Review,* **35**(2), pp.265-293

EDRM (2012) *IG Reference Model.* Version 3.0. [online]. [Accessed 15 March 2016]. Available at: http://www.edrm.net/projects/igrm

Education Research (2010) *Oral History: a Viable Methodology for 21st Century Educational Administration Research: National Impact*, Online Education. [online]. [Accessed 26 August 2015]. Available at: http://education-research-today.blogspot.co.uk/2009/07/oral-history-viable-methodology-for.html

Edwards, E. (2015) Increase seen in law suits for failing to protect personal data. *Irish Times.* [online]. 26 March. [Accessed 31 May 2015]. Available at: http://www.irishtimes.com/business/increase-seen-in-law-suits-for-failing-to-protect-personal-data-1.2154537

Endicoytt-Popuvsky, B. (2003) Ethics and teaching information assurance. *Security & Privacy.* [online]. *IEEE.* **1**(4), pp.65,67. July-August. doi: 10.1109/MSECP.2003.1219073. [Accessed 31 May 2015]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1219073&isnumber=27399

Ensor, C. (2011) *Presentation to BCS Security Community of Expertise (SCoE) on IA Professionalisation*

Esser, K.J. (2005) *Beyond the Preoccupation with Certification & Accreditation: A Guide to Conducting IA Systems Engineering during the Development of Tactical Systems.* [online]. GIAC Security Essentials Certification (GSEC), Practical Assignment. Version 1.4c. Option 1. 10 January. [Accessed 16 August 2015]. Available at: http://www.sans.org/reading_room/whitepapers/bestprac/preoccupation-certification-accreditation_1569

Evans, L. (2002) *Reflective Practice in Educational Research* (London, Continuum)

Evans, L. (2008) Professionalism, professionality and the development of education professionals. *British Journal of Educational Studies*, **56**(1). pp.20-38. [Accessed 21 April 2017]. Available at: http://eprints.whiterose.ac.uk/4077/2/Professionalism_professionality_and_the_development_of_educational_professionals_version_submitted_to_BJES.pdf

ETS (2001) *ETA 185, Convention on Cybercrime*

EURIM (2007) *EURIM investigation, Cyber-Crime Investigation and Enforcement*, D1.2

European Banking Authority (EBA) (2014) *Final guidelines on the security of internet payments*. EBA/GL/2014/12_Rev1. [online]. [Accessed 14 March 2016]. Available at: https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+(Guidelines+on+the+security+of+internet+payments)_Rev1

European Commission (2001) *Network and InfoSec: Proposal for a European Policy Approach.* COM(2001)298

Evetts, J. (2003) The sociological analysis of professionalism: occupational change in the modern world, *International Sociology*, **18**(2), pp.395–415

Evetts, J. (2006) Introduction: Trust and professionalism: challenges and occupational changes, *Current Sociology*, **54**(4), pp.515-531

Evetts, J. (2014) The concept of professionalism: Professional work, professional practice and learning. In *International handbook of research in professional and practice-based learning*, Springer Netherlands, pp.29-56

Ezingeard, J.-N., McFadzean, E. and Birchall, D. (2007) Mastering the art of corroboration: A conceptual analysis of IA and corporate strategy alignment. *Journal of Enterprise Information Management*. [online]. **20**(1), pp.96–118. [Accessed 27 February 2011]. Available at: http://www.emeraldinsight.com/journals.htm?articleid=1587879&show=html

Fafinski, S. and Minassian, N. (2008) *Garlik UK Cybercrime report*, with 1871 Ltd

Farrell, S. (2016) *TalkTalk counts costs of cyber-attack.* The Guardian. [online]. 2 February. [Accessed 11 March 2016]. Available at: http://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave

Fenz, S., Goluch, G., Ekelhart, A., Riedl, B. and Weippl, E. (2007) InfoSec Fortification by Ontological Mapping of the ISO/IEC 27001 Standard, *Dependable Computing*, PRDC, 13th Pacific Rim International Symposium, pp.381-388, IEEE

Ficenec, J. (2011) *What is The National Archive for: history and purpose.* [online]. [Accessed 20 April 2011]. Available at: http://ht.ly/4E2DL

Financial Times (2016) *People have had enough of experts*, [online]. [Accessed 7 May 2017]. Available at: https://www.ft.com/content/3be49734-29cb-11e6-83e4-abc22d5d108c

Fisher, C. (2007) *Researching and Writing a Dissertation – A Guidebook for Business Students*, 2nd edition, Essex: Pearson Education Limited

Fisher, N. (2010) *Evolution of Conflict - Views of The Future Seen From The Past and The Present: The Role of Information and its Infrastructure in Conflict*, World Defence Systems, Volume **1**

Fitzgerald, B. (2003) Informing each other: Bridging the gap between researcher and practitioners*, Informing Science*, Volume **6**, pp.13-19

Fitzgerald, T. (2012) *InfoSec Governance Simplified: From the Boardroom to the Keyboard*, Florida: CRC Press

Flechais, I., Riegelsberger, J. and Sasse, A. M. (2005) Divide and Conquer: The role of trust and assurance in the design of secure socio-technical systems, *New Security Paradigms Workshop*, ACM

Florencio, D. and Herley, C. (2011) *Sex, Lies and Cyber-crime Surveys*, Microsoft Research. Redmond, WA: Microsoft. [online]. [Accessed on 10 August 2011]. Available at: http://research.microsoft.com/pubs/149886/SexliesandCybercrimeSurveys.pdf

Forbes (2017) *Over 60% Of UK Businesses Lack Any Real Cyber Security,* Forbes online, 28 April 2017. [Accessed on 4 May 2017]. Available at: https://www.cybersecurityintelligence.com/blog/over-60-of-uk-businesses-lack-any-real-cyber-security-2358.html

Forrester (2015) *IG: Not Product, Not a Technology, Not a market.* [online] [Accessed 21 September 2015]. Available at: http://blogs.forrester.com/cheryl_mckinnon/15-01-14-information_governance_not_a_product_not_a_technology_not_a_market

Fortune (2011) *An Accident Waiting to Happen - the story on BP's oil spill in the Gulf*

Fox, J.M. (2003) *IA and the Defense in Depth: A study of InfoSec Warriors and InfoSec Cowboys.* Master of Military Art Thesis, Fort Leavenworth, Kansas. [online]. [Accessed 2 February 2011]. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA416561, or http://cgsc.contentdm.oclc.org/cdm4/item_viewer.php?CISOROOT=/p4013coll2&CISOPTR=60

Fox, M.L. (2015) *Dot Everyone,* The Richard Dimbleby Lecture. [online]. March. [Accessed 55 October 2015]. Available at: http://doteveryone.org.uk/

Fox, M., Martin, P. and Green, G. (2007) *Doing practitioner research*. Sage. ISBN: 978-1-4129-1234-1

Frank, U. (2006) *Evaluation of Reference Models.* In P. Fettke & P. Loos, (eds.) *Reference Modelling for Business Systems Analysis,* pp.118-140, Idea Group. [online]. [Accessed 2 May 2015]. Available at: http://www3.dsi.uminho.pt/rmac/privatefiles/papers/2007_RMBSAbook_DuarteFernandesMachado-idea.pdf

FRC (2005) *Guidance on Audit Committees (The Smith Guidance),* Financial Reporting Council. [online]. [Accessed 6 March 2011]. Available at: http://www.frc.org.uk/documents/pagemanager/frc/Smith%20Report%202005.pdf

Friedman, A. (2006) *Strengthening professionalism: Ethical competence as a path toward the public good*. Production Values: Futures for professionalism. Ed. John Craig. Demos

FSA (2008) *Data Security in Financial Services, Firms' controls to prevent data loss by their employees and third-party suppliers*, Financial Services Authority, Financial Crime and Intelligence Division. [online]. [Accessed 7 March 2011]. Available at: http://www.fsa.gov.uk/pubs/other/data_security.pdf

Furnell, S. (2011) Securing a Good Degree?, *IISP Pulse Magazine*, Spring, Issue 5

Gable, G.G. (1994) Integrating case study and survey research methods: an example in IS. *European Journal of IS.* **3**(2), pp.112–126

Galitz, W.O. (2007) *The Essential Guide to User Interface Design - An Introduction to GUI Design, Principles and Techniques.* 3rd edition. John Wiley & Sons

Galliers, R. (1985) *In search of paradigm for IS research.* In Mumford, E., Hirschheim, R., Fitzgerald, G. and Wood-Harper, T. (eds.) *Research Method in IS.* North-Holland: Elsevier Science Publishers, pp.271–284

Garfinkel, S. (1995) *PGP: Pretty Good Privacy*, Sebastopol, CA: O'Reilly & Associates, Inc.

Gartner (2010) *What is IG? And Why is it so Hard?* Gartner Blog Network: Debra Logan. [online].11 January. [Accessed 24 March 2016]. Available at: http://blogs.gartner.com/debra_logan/2010/01/11/what-is-information-governance-and-why-is-it-so-hard/

Gashi, I., Stankovic, V. and Turkay, C. (2015) *How Secure are Your Systems? Quantitative and Qualitative Assessment of Digital Security*

Gericke, A., Fill, H. G., Karagiannis, D. and Winter, R (2009) Situational Method Engineering for Governance, Risk and Compliance Information Systems. *Proceedings of the 4th International Conference on Design Science Research in Information Systems and Technology.* DESRIST '09. 24:1-24:12. ACM, New York, USA. [online]. [Accessed 2 May 2015]. Available at: http://www.researchgate.net/profile/Hans-Georg_Fill/publication/44939592_Situational_Method_Engineering_for_Governance_Risk_and_Compliance_Information_Systems/links/0fcfd510f7da80f9a7000000.pdf

Gilbert, N. (2008) *Researching Social Life,* 3rd edition, London: Sage

Gilderhus, M.T. (2006) *History and Historians: A Historiographical Introduction,* 6th edition, Pearson Education

Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R. and MacWillson, A. (2011) InfoSec and Privacy – Rethinking Governance Models. In *Communications of the Association for Information Systems (CAIS).* [online]. **28**(1), Article 33, pp.561-570. May. [Accessed 14 September 2015]. Available at: https://www.icaew.com/~/media/corporate/archive/files/technical/information%20technology/business%20systems%20and%20software%20selection/making%20information%20systems%20work/cais%20security%20and%20governance%20final%20article.ashx

Glaser, B.G. (1998) *Doing Grounded Theory - Issues and Discussions*. Sociology Press

Glass, R.L. (1998) *Software Runaways: Lessons Learned from Massive Software Project Failures*, New Jersey: Prentice Hall

Glyck, B. (2011) *Why the government IT strategy needs to become irrelevant.* Computer Weekly Editor's Blog. [online]. 15 April. [Accessed 18 April 2011]. Available at: http://www.computerweekly.com/blogs/editors-blog/2011/04/

Goodell, J. (1996) *The Cyberthief and the Samurai, The true story of Kevin Mitnick and the man who hunted him down*, New York: Dell Publishing

Gothard, P. (2016) GCHQ admits £1bn spend on cyber security 'hasn't worked'. *Computing.* [online]. 7 March. [Accessed 9 March 2016]. Available at: http://www.computing.co.uk/ctg/news/2449902/gchq-admits-gbp1bn-spend-on-cyber-security-hasn-t-worked?utm_medium=email&utm_campaign=CTG.All.A.LU_15&utm_source=CTG.DCM.Live_Updates

Grand, J. (1998) *Hackers Testifying at the United States Senate.* L0pht Heavy Industries. [online]. [Accessed 5 October 2015]. Available at: https://www.youtube.com/watch?v=VVJldn_MmMY

Grec, S. (2011) *IA versus InfoSec.* NovaInfosec Blog. Salvador "Grecs" Grec

Gregory, R. W. (2011) Design Science Research and the Grounded Theory Method: Characteristics, Differences and Complementary Uses. *Theory-Guided Modelling and Empiricism in Information Systems Research.* Berlin: Springer

Gross, B. (2015) *The single biggest reasons start-ups succeed.* TED Talk. [online]. [Accessed 23 September 2015]. Available at: https://www.ted.com/talks/bill_gross_the_single_biggest_reason_why_startups_succeed?language=en

Grupe, F.H., Garcia-Jay, T. and Kuechler, W. (2003) *Is it time for an IT Ethics Program?* pp.101-110

Guangco, C. (2007) Mind the Gap: A Critical Review of the IS Research and Practice Relationship. *iSChannel* **2**(1). [online]. [Accessed 14 September 2015]. Available at: http://www.lse.ac.uk/management/documents/--NEW--/research/is-channel/iSChannel-Volume-2.pdf

Guardian (2015) *Apple removes malicious programs after first major attack on app store*, The Guardian. [online]. 21 September. [Accessed 22 September 2015]. Available at: http://www.theguardian.com/technology/2015/sep/21/apple-removes-malicious-programs-after-first-major-attack-on-app-store

Guba, E.G. and Lincoln, Y.S. (1994) *Competing paradigms in qualitative research*. Ch 6 In: Denzin and Lincoln (1994) *Handbook of Qualitative Research*, USA: Sage Publishers

Hackett, R. (2015) *'Security has failed': Exclusive preview of RSA president's conference keynote.* [online]. April. [Accessed 7 May 2015]. Available at: http://fortune.com/2015/04/21/rsa-conference-amit-yoran-keynote/

Hall, K. (2011a) Security sponges up public sector ICT project budgets and hampers agility, *Computer Weekly*, Issue 8, p.8

Hall, K. (2011b) *Exclusive Interview: Deputy government CIO Bill McCluggage on the new government IT strategy.* [online]. 1 April. [Accessed 18 April 2011]. Available at: http://www.computerweekly.com/Articles/2011/04/01/246129/Exclusive-interview-Deputy-government-CIO-Bill-McCluggage-on-the-new-government-IT.htm

Hammersley, M. and Paul Atkinson, P. (2007) *Ethnography, principles in practice.* 3rd edition. Abingdon, Oxon: Routledge Taylor & Francis Group

Hampton, P. (2005) *Reducing administrative burdens: effective inspection and enforcement* (The Hampton Review). HM Treasury. Norwich: HMSO

Hamre, J. (1998) IA and The New Security Epoch. *USIA Electronic Journal.* November

Hancock, S. (2015) *European regulation shakes up online payments security*, Computer Weekly [online]. [Accessed 3 October 2015]. Available at: https://www.7safe.com/about-us/news/details/2015/08/06/european-regulation-shakes-up-online-payments-security

Hellawell, S. and Mulquin, M. (2000) *Putting IT into Practice: New Technology and the Modernising Agenda*, IS Communications Ltd, I&DeA, IBM, January

Heller, M. (2015) *Security ethics survey shows honesty is a tricky business*. [online]. 13 May. [Accessed 25 September 2015]. Available at: http://searchsecurity.techtarget.com/news/4500246224/Security-ethics-survey-shows-honesty-is-a-tricky-business?utm_medium=EM&asrc=EM_ERU_42840865&utm_campaign=20150514_ERU%20Transmission%20for%2005/14/2015%20(UserUniverse:%201522338)_myka-reports@techtarget.com&utm_source=ERU&src=5388751

Helsby, G. (1996) Professionalism in English secondary schools. *Journal of Education for Teaching.* **22**(2), pp.135 -148

Hercock, R.G. (2009) *Cohesion: The Making of Society*, Marston Gate: Lulu Press / Amazon

Herold, R. and Rogers, M.K. (2010) *Encyclopaedia of IA*, Boca Raton, Fla.: Auerbach Publications

Herrmann, D.S. (2002) *A practical guide to Security Engineering and IA*, Florida: CRC Press / Auerbach Publications

Higgs, D. (2003) *Review of the role and effectiveness of non-executive directors*. [online]. January. [Accessed 6 March 2011]. Available at: http://www.berr.gov.uk/files/file23012.pdf

Hinson, G. (2007) The State of IT Auditing in 2007, *EDPACS*, **36**:1, pp.13-31

Holland, J. H. (2006). Studying Complex Adaptive Systems. *Journal of Systems Science and Complexity.* **19**(1): 1-8. [online]. [Accessed 27 November 2011]. Available at: http://hdl.handle.net/2027.42/41486

Hollway, W. and Jefferson, T. (2008) *The free association narrative interview method*. In: Given, Lisa M. (ed.) The SAGE Encyclopedia of Qualitative Research Methods. Sevenoaks, California: Sage, pp.296-315. [online]. [Accessed 27 November 2011]. Available at: http://oro.open.ac.uk/15410/1/H&J4FANImeth08.pdf

Holt, A.L. (2013) *Governance of IT: An executive guide to ISO/IEC 38500,* BCS Learning and Development Ltd: Swindon, England

Holtham, C. (2015) IM – the fundamental philosophy, *IRMS Bulletin*, **186**, p.13

Hong, KS, Chi YP, Chao, LR and Tang, JH (2003) *An integrated system theory of information security management,* Information Management & Computer Security, **11**(5), pp.243-248

Hoo, K.J. (2000) "*How Much Is Enough? A Risk-Management Approach to Computer Security*", (Consortium for Research on InfoSec and Policy [CRISP]), in IAAC April 2003 – *Engaging the Board: Corporate Governance & IA*, Aarti Anhal, Stephanie Daman, Kevin O'Brien and Andrew Rathmell

Hotten, R. (2015) *Volkswagen: The scandal explained.* BBC News. [online]. 10 December. [Accessed 24 December 2015]. Available at: http://www.bbc.co.uk/news/business-34324772

Howard, D. and Prince, K. (2011) *Security 2020 Reduce Security Risks This Decade.* Indianapolis: Wiley Publishing Inc.

Hulme, G. (2012) *Bad System Design Begs for Circumvention*, ISSA International Conference blog post. [online]. [Accessed 6 September 2015]. Available at: http://www.issa.org/blogpost/906761/152809/Bad-System-Design-Begs-for-Circumvention

Humes, J. (2003) *Nuts 'n bolts Leadership – "How To Strategies and Practical Tips for Leaders at ALL levels".* Texas: The WALK THE WALK Company, p.9

Hutton, N. (2008) IA: 'must try harder'. *ITadviser.* pp.16-17. [online]. [Accessed 7 February 2011]. Available at: http://www.360is.com/downloads/ncc-mag-issue-56-360is.pdf

I&DeA (2003) *Delivering service improvement through addressing*, The National Land & Property Gazetteer

IATAC (2007) *Software Security Assurance – A State of the Art Report (SOAR)*, p.3-5, Virginia, USA

IBM (2005) *IBM WebSphere Information Integration platform delivers information you can trust,* USA: IBM Software Group

IBM (2013) *Making Leaders Successful Every Day: Information and Integration Governance Imperative.* A commissioned study conducted by Forrester Consulting on behalf of IBM. Slide 16. [online]. [Accessed 15 March 2016]. Available at: https://www-950.ibm.com/events/wwe/grp/grp004.nsf/vLookupPDFs/Make%20Leaders%20Successful%20Every%20Day_Michelle%20Goetz/$file/Make%20Leaders%20Successful%20Every%20Day_Michelle%20Goetz.pdf

ICAEW (1999) (Turnbull Report) *Internal Control: Guidance for Directors on the Combined Code*

IISP (2016) *Security market trends and predictions: from the 2015 member survey.*

IISP (2017) *Skills Framework* [online]. [Last accessed 4 February 2018]. Available at: https://www.iisp.org/imis15/iisp/About_Us/Our_Skills_Framework/iispv2/Accreditation/Our_Skills_Framework.aspx?hkey=e77a6f03-9498-423e-aa7b-585381290ec4

Iivari, J., Hirschheim, R. and Klein, H.K. (1998) A Paradigmatic Analysis Contrasting IS Development Approaches and Methodologies. *IS Research.* **9**(2), pp.164–193

IMA (2014) *Upgrading Risk management and Internal Control in Your Organization.* IMA's Annual Conference & Exposition. Presentation by McNally, J.S., Soup C. and Tophoff, V.H., IFAC. PowerPoint presentation. [online]. [Accessed 15 March 2016]. Available at: http://www.slideshare.net/IFAC_Multimedia/ima-june-2014conferenceupgradingrmicsessiondeckfinal

Information Assurance Advisory Council (IAAC) (2000a) *Protecting the Information Society.* Briefing Paper (BP) 01. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000b) *UK Policy Developments*. BP02. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000c) *E-Business Risks report* following seminar held on 17 May 2000, paper includes "Risks in the Information Economy" by Dr Oliver Sparrow, Chatham House Forum

IAAC (2000d) *US Policy Developments*. BP03. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000e) *The European Union's Approach to IA and CIP Policy*. BP04. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000f) *International Organisations and CIP Policy*. BP05. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000g) *Russian and Chinese Policy Overviews*. BP06. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000h) *France and German Policy Overviews.* BP07. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000i) *North European Policy Overviews.* BP08. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000j) *CIP Policy Developments in Ireland. The Netherlands, Belgium and Switzerland.* BP09. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000k) *CIP Policy Developments in Italy, Spain, Portugal and Greece*. BP10. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000l) *Australian and Canadian Policy Overviews*. BP11. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000m) *Pacific Rim Policy Overview.* BP12. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000n) *Israel, The Arab States and North Africa CIP Policy Overview.* BP13. [online]. [Accessed 10 May 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2000o) *Risk Analysis – a Review by the IAAC Dependencies & Risk Working Group (DRWG)*

IAAC (2001a) *Critical Infrastructure Protection and Crisis Management in Britain,* BP14

IAAC (2001b) *Protecting Online Financial Services through New International and National Supervisory Regulations)*. BP15

IAAC (2001c) *Enabling business through IA, Protection Critical Information Infrastructures*. Presentation by Dr Andrew Rathmell

IAAC (2001d) *Military Dependency on Civilian Infrastructures*. BP16

IAAC (2001e) *The Costs of Cybercrime.* BP17. [online]. [Accessed 16 March 2016]. Available at: http://www.iaac.org.uk/library-resources/library/archive/briefings/

IAAC (2001f) *Technical Security Issues and Trends for Critical Infrastructure Protection*. BP18

IAAC (2001g) *The Domain Name Systems (DNS) and the Protection of Corporate Identity on the Internet*. BP19

IAAC (2001h) *Establishing Trust in Cyber-Space: Regulation or Self-Regulation.* BP20

IAAC (2001i) *Raising Awareness of IA*

IAAC (2001j) *A Safety Critical Software Approach to InfoSec.* BP21

IAAC (2001k) *Building a Safe and Secure Information Society: UK Public Policy Requirements, IAAC Recommendations*

IAAC (2001l) *Information Flow in IA.* BP22

IAAC (2001m) *Information Sharing Review: Sharing is Protecting – Policy Paper.* [Last accessed 10 May 2016]. Available at: http://www.iaac.org.uk/media/1251/info_sharingv3.pdf

IAAC (2001n) *IA and Good Corporate Governance.* BP23

IAAC (2002a) *Identity Theft Highlights the Importance of 'Data Responsibility'*. BP24

IAAC (2002b) *US Critical Infrastructure Protection Policies since 11th September.* BP25

IAAC (2002c) *Will Broadband Rollout undermine InfoSec?* BP26

IAAC (2002d) *Protecting the Digital Society: A Manifesto for the UK*. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1138/iaacmanifesto270202.pdf

IAAC (2002e) *CYBER HOOD WATCH: Empowering the Digital Citizen.* InfoSec in the Public Sector. Presentation

IAAC (2002f) *Dealing with Cybercrime.* BP27

IAAC (2002g) *Engaging the Board: Corporate Governance & Information Risk, IAAC Recommendations.* [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1141/cg-recommendations-paper.pdf

IAAC (2002h) *Do IT Security Consultants need a Licence?* BP28

IAAC (2002i) *Should OFCOM regulate InfoSec?* BP29

IAAC (2002j) *Digital Identities*. BP30

IAAC (2002k) *Dealing with Cyber-terrorism*. BP31

IAAC (2002l) *How can you embed IA in the Board Risk Agenda?* BP32

IAAC (2002m) *Insuring Digital Risk: A roadmap for Action,* Prepared by John Ridd and RAND Europe. [online]. October. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1143/ridd_insurance_final.pdf

IAAC (2002n) *Promoting a Culture of InfoSec in Europe.* BP34. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1214/paper34.pdf

IAAC (2003a) *Insurance & IRM.* BP35

IAAC (2003b) *Deterring Cyber-crime: Lessons for the future.* BP36. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1216/paper36.pdf

IAAC (2003c) *Building In Security.* BP37. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper37.pdf

IAAC (2003d) *Cyber Terrorism: An Emerging Threat.* BP38. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper38.pdf

IAAC (2003e) *The Insider Threat: The Enemy Within.* BP39. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper39.pdf

IAAC (2003f) *Reacting to Cybercrime.* BP40. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper40.pdf

IAAC (2003g) *Information sharing: A 'no brainer' approach to Improved Risk Management.* BP41. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper41.pdf

IAAC (2003h) *Measuring the Benefits of InfoSec to Improved Risk Management.* BP42. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper42.pdf

IAAC (2003i) *Who is responsible for investigating e-Crime?* BP43. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper43.pdf

IAAC (2003j) *Awareness Raising in Europe.* BP44. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper44.pdf

IAAC (2003k) *Understanding Trust.* BP45. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1217/paper45.pdf

IAAC (2003l) *The Draft Civil Contingencies Bill.* BP46

IAAC (2003m) *Director's IA Network (*DIAN) - IA Maturity Scorecard

IAAC (2004a) *Deception in Computer Networked Defence.* BP47. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1228/paper47.pdf

IAAC (2004b) *Assured International Passenger Name Record Data.* BP48. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1229/paper48.pdf

IAAC (2004c) *InfoSec and the Ordinary User.* BP49. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1230/paper49.pdf

IAAC (2004d) *Reform of the Computer Misuse Act 1990.* BP50. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1231/paper50.pdf

IAAC (2004e) *Meeting public sector IA requirements.* BP51. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1232/paper51.pdf

IAAC (2004f) *Teaching the Teachers.* BP52. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1233/paper52.pdf

IAAC (2004g) *Transnational Co-operation in the fight against cyber-crime.* BP53. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1234/paper53.pdf

IAAC (2004h) *Revising Business Continuity.* BP54. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1235/paper54.pdf

IAAC (2004i) *Delivering IA: What needs to be done?* BP55. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1236/paper55.pdf

IAAC (2004j) *The changing cyber-crime threat.* BP56. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1237/paper56.pdf

IAAC (2004k) *The FoIA as a path to good IA.* BP57. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1238/paper57.pdf

IAAC (2005a) *Emergent European frameworks for Network and InfoSec.* BP58. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1239/paper58.pdf

IAAC (2005b) *Identity Management & IA, Executive Summary.* BP59. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1240/paper59.pdf

IAAC (2005c) *IA and the SME.* BP60. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1241/paper60.pdf

IAAC (2005d) *Realising the Cyber-Trust and Crime Prevention.* BP61. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1242/paper61.pdf

IAAC (2005e) *Cyber Hood Watch.* BP62. [online]. [Accessed 14 March 2016]. Available at: http://www.iaac.org.uk/media/1243/paper62.pdf

IAAC (2007a) *Government's Role in Identity Assurance.* BP63. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1244/paper63.pdf

IAAC (2007b) *National IA Strategy.* BP64. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1245/paper64.pdf

IAAC (2008a) *The Needs and Concerns of the Citizen.* BP65. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1246/paper65.pdf

IAAC (2008b) *How UK Government can Gain Citizen Support.* BP66. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1247/paper66.pdf

IAAC (2008c) *Citizen Control.* BP68. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1247/paper68.pdf

IAAC (2008d) *Digital Identity Governance Framework.* BP69. [online]. [Accessed 8 September 2015]. Available at: http://www.iaac.org.uk/media/1248/paper69.pdf

IAAC (2010) *Annual Symposium presentation by Professor Phil Hutchinson,* Shrivenham: Cranfield University. 8 September. London

IAAC (2017) *The Profession: Understanding careers and professionalism in cyber security*, February 2017, Swindon

Information Governance Initiative (IGI) (2014a) *IGI* description of IG. [online]. [Accessed 22 September 2015]. Available at: http://iginitiative.com/

IGI (2014b) *IGI Annual Report 2014: IG Goes to Work.* [online]. August. [Accessed 26 April 2015]. Available at: http://iginitiative.com/igi-publishes-2014-annual-report/

IGI (2014c) *IGI Annual Report 2014: The Facets of IG.* [online]. [Accessed 15 March 2016]. Available at: http://ethicalboardroom.com/wp-content/uploads/2014/12/Baron_figure1.jpg

Information Security Forum (ISF), (ISC)² and ISACA (2010) *Principles for InfoSec Practitioners: An overview,* ISF Limited

ISF (2013) *The Standard of Good Practice for InfoSec.* [online]. Available at: https://www.securityforum.org/research/publicdownload2013sogp/

Inspired (2017) Inspired Careers website [online]. [Accessed 10 May 2017]. Available at http://www.inspiredcareers.org/browse-careers/cyber-security/

Institute of Internal Auditors (IIA) (2009) *IIA Position Paper: The Role of Internal Auditing in Enterprise-Wide Risk Management*. ERM PP. p.4 [online]. January. [Accessed 15 March 2015]. Available at: https://www.iia.org.uk/media/78513/the_role_of_internal_audit_in_enterprise_risk_management.pdf

IIA (2010) *Applying COSO's ERM — Integrated Framework*

IIA (2013) *IIA Position Paper: The Three Lines of Defense in Effective Risk Management and Control.* USA: Florida. [online]. January. [Accessed 15 March 2016]. Available at: https://na.theiia.org/standards-guidance/Public%20Documents/PP%20The%20Three%20Lines%20of%20Defense%20in%20Effective%20Risk%20Management%20and%20Control.pdf

Ilieş, I.M. and Boaru, G. (2011) Information assurance-intelligence-information superiority relationship within NATO operations. *Journal of Defense Resources Management (JoDRM)*, **2**(2), pp.111-120

Internet Crime Forum (ICF) (2003) *Reform of the Computer Misuse Act 1990*, Legal Subgroup

ICF (2005) *The Public Private Boundary on the Internet*, Legal Subgroup

IPCC (2008) Independent Police Complaints Commission *Independent Investigation into the HMRC* loss. [online]. [Accessed 7 February 2011]. Available at: http://www.ipcc.gov.uk/news/Pages/pr_250608_missing_hmrc_data_cds.aspx

Iron Mountain (2014) *A Practical Guide to IG.* White Paper. p.11

ISACA (2009) *An Introduction to the Business Model for InfoSec (BMIS).* [online]. p.13. Figure 2. Overview of BMIS. Illinois: ISACA. (c) 2010, ISACA(R) All rights reserved, Used by permission (June 2012) [Accessed on 8 July 2012]. Available at: www.isaca.org/bmis, http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

ISACA (2010a) *The BMIS.* Illinois: ISACA. [online]. [Accessed 15 March 2016]. Available at: http://www.emi-tuv.hu/uploads/images/133715505073288047021 9/isaca-bmis-2010.pdf

ISACA (2010b) *COBIT 5.0, Design Paper Exposure Draft*

ISACA (2014) *Cybersecurity Report: The Growing Cybersecurity Skills Crisis – Addressing the conflict of too many threats and too few skilled professionals*. [online]. [Accessed 3 May 2015]. Available at: http://www.isaca.org/cyber/Documents/Cybersecurity-Report_pre_Eng_0414.pdf

(ISC)² (2011d) *The 2011 ISC2 Global InfoSec Workforce Study.* Frost & Sullivan. [online]. [Accessed 26 April 2015]. Available at: https://www.isc2.org/uploadedfiles/industry_resources/fs_wp_isc%20study_020811_mlw_web.pdf

(ISC)² (2013a) *The 2013 ISC2 Global InfoSec Workforce Study.* Frost & Sullivan. [online]. [Accessed 26 April 2015]. Available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf

(ISC)² (2015g) *The 2015 ISC2 Global InfoSec Workforce Study.* Frost & Sullivan. [online]. [Accessed 26 April 2015]. Available at: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

(ISC)² (2015h) *Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees: A resource for course designers and accreditors*. Version 1.1. With CPHC. [online]. [Accessed 7 September 2015]. Available at: https://www.isc2.org/uploadedfiles/(isc)2_public_content/emea_content/cybersecurity-principles-learning-outcomes-whitepaper.pdf

(ISC)² (2015h) *Official* (ISC)² *Guide to the CISSP CBK*. 4th edition. Florida: Auerbach / CRC Press

ISM (2010) UK to spend £650m on new National Cyber Security Programme, *InfoSecurity Magazine.* [online]. 20 October. [Accessed 13 March 2016]. Available at: http://www.infosecurity-magazine.com/news/uk-to-spend-650m-on-new-national-cyber-security/

ISM (2015) 80% of companies had a security incident in 2015. *InfoSecurity Magazine.* Tara Seals. [online]. [Accessed 15 March 2016]. Available at: www.infosecurity-magazine.com/news/80-companies-had-a-security/

ISM (2016) *Cybersecurity leadership requires seat at the executive table*. In *Information Security Magazine.* December 2016. **18**(10), p.12

IT Compliance Institute (2010) *IT Governance and Strategy.* Compliance Insight: IT Audit Checklist Series

IT Governance Institute (ITGI) (2000) *COBIT: Governance, Control and Audit for Information and Related Technology.* 3rd edition. Illinois: ISACA

ITGI (2012) *InfoSec Governance: Guidance for Boards of Directors and Executive Management,* 2nd edition, Illinois: ISACA

Jaffray, P. (2016) *The Breacher Report*

Johnson, R. and Christensen, L. (2005) *Overview of the Historical Research Process*. [online]. [Accessed 16 August 2015]. Available at: http://www.southalabama.edu/coe/bset/johnson/oh_master/Ch14/Fig14-04.pdf

Jones, N. (2009) *Building in … InfoSec, Privacy and Assurance – A high-level roadmap.* London: Cyber Security Knowledge Transfer Network

Joseph Rowntree Reform Trust Ltd (2009) *Database State.* York: Joseph Rowntree Reform Trust Ltd [online]. [Accessed 5 September 2015]. Available at: http://www.jrrt.org.uk/sites/jrrt.org.uk/files/documents/database-state.pdf

Kabay, M.E. (undated), *On Writing.* [online]. [Accessed 5 May 2015]. Available at: http://www.mekabay.com/methodology/writing_undergrad.htm

Kabay, M.E. (2002) Using Social Psychology to Implement Security Policies. *Computer Security Handbook.* [online]. Chapter 35. 4th edition. John Wiley & Sons. [Accessed 12 Jan 2015]. Available at: http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf

Kahn, R.A. and Blair, B.T. (2009) *Information Nation: Seven Keys to Information Management Compliance.* p.14. Indianapolis: Wiley

Kaplan, R.S. (2008) Conceptual foundations of the balanced scorecard. In *Handbooks of management accounting research.* **3**, 1253-1269. [Draft working paper from Harvard Business School, Harvard University, 2010]

Karas, T.H., Moore, J.H. and Parrott, L.K. (2008) *Metaphors for cyber security*. Sandia Report SAND2008-5381. Sandia Labs, NM

Keen, P.G.W. (1980) *MIS Research: Reference Disciplines and a Cumulative Tradition*. Sloan School of Management. Massachusetts Institute of Technology

Kelly, L. (2010) *Making a return on IT security investment.* Blog post [online]. Undated. [Accessed 2 October 2015]. Available at: http://www.computerweekly.com/feature/Making-a-return-on-IT-security-investment

Kellogg Foundation (2004) *Using Logic Models to Bring Together Planning, Evaluation, and Action: Logic Model Development Guide*. Michigan. [Accessed 11 November 2017]. Available at: https://ag.purdue.edu/extension/pdehs/Documents/Pub3669.pdf

Kerckhoffs, A. (1883) La cryptographie militaire. *Journal des sciences militaires*, *9*, p.538

Kesar, S. (2011) Is Cybercrime one of the weakest links in Electronic Government? *Journal of International Commercial Law and Technology.* [online]. **6**(4). [Accessed 16 August 2015]. Available at: http://www.jiclt.com/index.php/jiclt/article/view/143

Kim, A.J. (2000) Maslow's Hierarchy of Needs applied to the online world. *Community Building on the Web.* Peachpit

King, S. (2008) *The Coleman Report - An Independent Review of Government IA.* [online]. [Accessed 6 February 2011]. Available at: http://www.computerweekly.com/blogs/stuart_king/2008/07/coleman-report.html

Kingova, K. (2013) *Securitization of Cyber Space in the United States of America, the Russian Federation and Estonia*. [Accessed 12 March 2017]. Available at: http://www.etd.ceu.hu/2013/klingova_katarina.pdf

Koenig, D.R. (2012) *Governance Reimagined: Organizational Design, Resign, and Value Creation.* New Jersey: John Wiley & Sons, Inc.

Kofsky, L. (2011) *What is InfoGov?* [online, no longer available]

Korah, D. (2006) *OSI Model* - Open system interconnection model. [online]. Picture created and shared by open commons. [Accessed 14 March 2016]. Available at: https://commons.wikimedia.org/wiki/File:Osi-model.png

Kovacich, G.L. (1998) *IS Security Officer's Guide, Establishing and Managing an IP Program.* p.2. Woburn: Butterworth-Heinemann

Kovacich, G.L. (2001) The Corporate IA Officer (CIAO). *Computers & Security.* **20**(4), pp.302-307

KPMG (2002) *Is Britain on Course for 2005, The third KPMG Consulting e-government survey.* April. (Originally published in Spring 2000)

KPMG (2010) *Survival of the Most Informed: GRC Comes of Age – How to Envision, Strategize, and Lead to Achieve Enterprise Resilience.* KPMG GRC Advisory. KPMG International Cooperative. [online]. [Accessed 20 September 2015]. Available at: https://www.kpmg.com/GR/en

Krause, M. and Tipton, H.F. (2004) *InfoSec Management Handbook*. 5th edition. Florida: Auerbach Publications. p.975

Lacey, D. (2009) *Human Factors in InfoSec. How to win over staff and influence business managers.* West Sussex: Wiley

Lacey, D. (2013a) Ditch the Triangle and use more technology. *David Lacey's IT Security Blog.* [online]. 20 January. [Accessed 2 October 2013]. Available at: http://tinyurl.com/aovaja3

Lacey, D. (2013b) *David Lacey on the Origins of ISO27k. in* The State of Security blog. Tripwire. [online]. 18 August. [Accessed 7 May 2015]. Available at: http://www.tripwire.com/state-of-security/regulatory-compliance/david-lacey-on-the-origins-of-iso27k/

Leach, J. (2003) *An Engineering Approach to the Design of Accurate and Reliable Security Systems*

Leech, T. (2016) *Three Lines of Defense vs. Five Lines of Assurance: Elevating the Role of the Board and CEO in Risk Governance,* presentation by Risk Oversight Solutions Inc., 31 May 2016

Leming, R. (2015) *6 IG Initiatives for 2015 – the Search for Information Treasure.* [online]. [Accessed 15 March 2016]. Available at: https://www.linkedin.com/pulse/6-information-governance-initiatives-2015-reynold-leming

Lewis, D. (2016) *What the All Writs Act of 1789 has to do with the iphone,* [online] 24 February 2017. [Accessed 28 January 2017]. Available at: http://www.smithsonianmag.com/smart-news/what-all-writs-act-1789-has-do-iphone-180958188/

Liles, S. (2011) *Draft: The myth of cyber space as a man-made domain.* [online]. [Accessed on 18 April 2015]. Available at: http://selil.com/archives/2311

Liles, S. and Kamali, R. (2006) An information assurance and security curriculum implementation. *Issues in Informing Science and Information Technology*, ***3***, pp.383-387

Lucas, E. (2015) Cyberphobia: Identity, Trust, Security and the Internet. London: Bloomsbury Publishing Ltd

Lukasik, S.J., Goodman, S.E. and Longhurst D.W. (2003) Protecting Critical Infrastructures Against Cyber-Attack. Adelphi Paper. **43**(359). London: Oxford University Press

Luo, D. (1997) Bifurcation theory and methods of dynamical systems. In Advanced Series in Dynamical Systems. Singapore: World Scientific

Lyons, S. (2016) Spotlight: 21st Century corporate defence. In The Risk Universe, August 2016, p.24

Maconachy, V., Schou, C., Ragsdale, D. and Welch, D. (2001) A Model for IA: An Integrated Approach. *Proceedings of the 2001 IEEE Workshop on IA and Security*. U.S. Military Academy. West Point, New York. [online]. [Accessed 8 July 2012]. Available at http://www.itoc.usma.edu/Workshop/2001/Authors/Submitted_Abstracts/paperW2C3(55).pdf and http://darpa.academia.edu/DanielRagsdale/Papers/762175/A_model_for_information_assurance_An_integrated_approach

Macrory, R.B. (2006) *Regulatory Justice: Making Sanctions Effective*

MacDonald, K.M. (1995) *The Sociology of the Professions*. London: Sage

Magee (2008) *Review of Criminality Information.* [online]. [Accessed 7 February 2011]. Available at: http://tna.europarchive.org/20080728093108/police.homeoffice.gov.uk/operational-policing/review-criminality-information/

Mansell, R. and Collins, B.S. (2005) *Trust and Crime in Information Societies.* DTI, Cheltenham: Edward Elgar

Marsh, S. (2003) *IAAC Workshop.* CSIA introductory presentation

Mason, R.O., McKenney, J.L. and Copeland, D.G. (1997a) *Developing an Historical Tradition in MIS Research.* MIS Quarterly

McBride, N. (2007) *The Death of Computing* (member view). [online]. January. [Accessed 2 October 2015]. Available at: http://www.bcs.org/content/ConWebDoc/9662

McCumber, J. (1991) IS Security: A Comprehensive Model. Paper presented at the *Proceedings of 14th National Computer Security Conference*. NIST, Baltimore, MD. Contains the McCumber Cube. Permission Granted. [online]. [Accessed 3 February 2011]. Available at: http://www.humanitarian.info/2008/03/25/pass-the-security-cube-aka-no-bullets-involved-part-3/; [Accessed 2 September 2015]. Available at: http://trygstad.rice.iit.edu:8000/Government%20Documents/NSTISS/NSTISSI4011Annex.rtf

McGraw, G. and Arce, I. (2010) *Software (In) Security: Cyber Warmongering and Influence Peddling.* [online]. 24 November. [Accessed 22 February 2011]. Available at: http://www.informit.com/articles/article.aspx?p=1662328

McFadzean, E. (2005) *The case for IA and Corporate Strategy Alignment,* Part 5, Henley Management College

McIlwraith, A. (2006) *InfoSec and Employee Behaviour: How to Reduce risk Through Employee Education, Training and Awareness,* Aldershot: Gower Publishing Limited

McKinsey (2009) Risk: Seeing around the corner, *McKinsey Quarterly,* article by Eric Lanmarre and Martin Pergler. [online]. [Accessed 14 September 2015]. Available at: http://www.mckinsey.com/insights/risk_management/risk_seeing_around_the_corners

McKnight, W.L. (2002) What is IA?. In *CROSSTALK The Journal of Defense Software Engineering.* Shim Enterprise, Inc. [online]. [Accessed 2 September 2015]. Available at: http://www.crosstalkonline.org/storage/issue-archives/2002/200207/200207-McKnight.pdf

McLuhan, M., Fiore, Q. and Agel, J. (1968) *War and peace in the global village.* Volume **127**. New York: Bantam books

Marks, N. (2011) *Marks on Governance Blog – Podcast on GRC and a Related Discussion Forum.* [online]. [Accessed 27 February 2011]. Available at: http://www.theiia.org/blogs/marks/index.cfm/post/Norman's%20Podcast%20on%20GRC,%20and%20a%20Related%20Discussion%20Forum

Meer, H. (2013) *Your company's security posture is probably horrible (but it might be OK).* thinkst applied research. [online]. [Accessed 5 October 2015]. Available at: http://blog.thinkst.com/2013/01/your-companies-security-posture-is.html

Meer, H. (2015) *the hard thing (about the hard things).* Presentation. [online]. thinkst applied research. [Accessed 5 October 2015]. Available at: https://www.troopers.de/media/filer_public/88/96/889669f0-f1cc-4170-bc94-24b9793875aa/thinkst-troopers-2015-no-notes.pdf

Mefford, J. (2014) *A Pathway to Principled Performance: The OCEG Capability Model's Approach to Integrated GRC.* [online]. [Accessed 15 March 2016]. Available at: http://www.meffordmultimedia.com/wp-content/uploads/2014/09/M3-A-Pathway-to-Principled-Performance-Jason-Mefford.pdf

Mezirow, J. (1991) *Transformative Dimensions of Adult Education*. San Francisco: Jossey-Bass

Microsoft (2002) *Building a Secure Platform for Trustworthy Computing*. White Paper. Security Compliance Management Toolkit. [online]. December. [Accessed 16 March 2016]. Available at: http://technet.microsoft.com/en-us/library/cc677002.aspx

Microsoft (2003) *Strategies for Fault-Tolerant Computing: The Availability Equation: People, Process, and Technology.* [online]. 22 January. [Accessed 16 March 2016]. Available at: https://msdn.microsoft.com/en-us/library/bb742373.aspx

Miles, M.B. and Huberman, A.M. (1994) *An Expanded Sourcebook Qualitative Data Analysis.* 2nd edition. London: Sage Publications

Miles, M.B. and Huberman, A.M. (2002) *The Qualitative Researcher's Companion.* London: Sage Publications

Miller, B. (2008) *Data Protection: House of Lords debates.* [online]. 12 June, 3:00 pm. [Accessed 7 February 2011]. Available at: http://www.theyworkforyou.com/lords/?id=2008-06-12a.724.5

Miller, D. (2013) *Maximising the Business Impact of IT: Importance of managing the total business experience.* School of Science and Technology. Middlesex University: London

Miller, D. (2015) Eliminating Waste. *Digital Leaders.* p.110. [online]. [Accessed 9 July 2015]. Available at: http://www.bcs.org/upload/pdf/eliminating-waste-150415.pdf

Millman, R. (2016) *UK firms at risk due to employees' lack of cyber-security awareness.* SC magazine. [online]. March. [Accessed 12 March 2016]. Available at: http://www.scmagazineuk.com/uk-firms-at-risk-due-to-employees-lack-of-cyber-security-awareness/article/481375/?DCMP=EMC-SCUK_Newswire&spMailingID=13911233&spUserID=MjMzNTY0ODgzNgS2&spJobID=740547867&spReportId=NzQwNTQ3ODY3S0

MIT Sloan (2011) *Theory X and Y; Organizational Development* (McGregor). [online]. [Accessed 6 August 2015]. Available at: http://mitsloan.mit.edu/faculty/spotlight/pioneered.php

Mooney, J. (2015) Standing In Data Breach Litigation: Lessons From 2014. *Law360.* [online]. January. [Accessed 31 May 2015]. Available at: http://www.law360.com/articles/608294/standing-in-data-breach-litigation-lessons-from-2014

Moreton, R. and Chester, M. (1997) *Transforming the business: The IT contribution.* Berkshire: McGraw-Hill

MORI (2001) *E-government Research Review: Research Report for the Audit Commission*

Mumford, E. and Beekman, G. (1994) *Tools for change & Progress.* The Netherlands: CSG Publications

Myers, M.D. (1997) Qualitative Research in IS. *MIS Quarterly.* **21**(2), pp.241–242

Nanton, T.J. (2004) *Achieving IA.* USAWC Strategy Research Project. US Army War college, Pennsylvania. [online]. [Accessed 24 June 2015]. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424379

National Association of Corporate Directors (NACD) (2001) *Presenting the InfoSec Case to the Board of Directors, Audit and Control*

National Audit Office (NAO) (2013) *The UK cybersecurity strategy: Landscape review.* Cross-government review. [online]. [Accessed 1 September 2015]. Available at: http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

National Computing Centre (NCC) (2004a) *Protect and Survive: Defending against Application Hacking.* October. Guidelines for IT Management. NCC Guidelines Number 289. Manchester: The NCC

National Defense Industrial Association (NDIA) (1998) *Information Assurance Study*. [online]. [Accessed 7 September 2015]. Available at: http://oai.dtic.mil/oai/oai?&verb=getRecord&metadataPrefix=html&identifier=ADA391445

Nige the Security Guy (2013) *Architecture Case Study - Part 1: Defence in Depth.* Blog. [online]. [Accessed 16 March 2016]. Available at: https://nigesecurityguy.wordpress.com/2013/06/28/architecture-case-study-part-1/

Nolan, R. L. (1973) *Managing the Computer Resource: A Stage Hypothesis*. In *Communications of the ACM.* **16**(7), p.399-405. [online]. [Accessed 16 August 2015]. Available at: http://cacm.acm.org/magazines/1973/7/11861-managing-the-computer-resource/abstract

Nolan, R.L. and McFarlan, F.W. (2005) IT and the Board of Directors. *Harvard Business Review.* [online]. [Accessed 3 October 2015]. Available at: http://www3.fsa.br/LocalUser/gestaoti/Ativ03%20NOLAN%202005%20%20Information%20Technology%20and%20the%20Board%20of%20Directors.pdf

Norris, M. (2015) *Between you and me: Confessions of a Comma Queen.* W.W. New York: Norton & Company

O'Brien, R. (2001) *Um exame da abordagem metodológica da pesquisa ação [An Overview of the Methodological Approach of Action Research].* In Roberto Richardson (Ed.), *Teoria e Prática da Pesquisa Ação [Theory and Practice of Action Research].* João Pessoa, Brazil: Universidade Federal da Paraíba. (English version). [online]. [Accessed 30 May 2002]. Available: http://www.web.ca/~robrien/papers/arfinal.html

Oakley, K. (2000) *eGovernment, an international study of online government.* Commissioned by Cable & Wireless Communications

OECD (1992) *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security.* Paris. ***Replaced by the 2002*** *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*. [online]. [Accessed 6 March 2011]. Available at: http://www.oecd.org/document/42/0,3746,en_2649_34255_15582250_1_1_1_1,00.html

OECD (2011) *OECD/IFP Project on "Future Global Shocks", "Reducing Systemic Cybersecurity Risk".* Peter Sommer. IS and Innovation Group. London School of Economics; Ian Brown, Oxford Internet Institute, Oxford University

OECD (2015) *G20/OECD Principles of Corporate Governance.* OECD Report to G20 Finance Ministers and Central Bank Governors

OCEG (2009a) *GRC Capability Model: Red Book*. Open Compliance and Ethics Group

OCEG (2015a) *GRC Maturity Survey: How the approach to GRC Strategy & Integration Affects Confidence.* [online]. April. [Accessed 2 May 2015]. Available at: http://www.oceg.org/resources/oceg-2015-grc-maturity-survey-report/

OCEG (2015b) *GRC Capability Model Element View.* Exposure Draft. OCEG Red Book GRC Capability Model: Achieving Principled Performance by integrating the governance, assurance and management of performance, risk and compliance. Version 3.0-Exposure. p.16

Oltsik, J. (2014) *The ESG Cybersecurity Maturity Model.* Enterprise Strategy Group. [online]. October. [Accessed 1 September 2015]. Available at: http://resources.idgenterprise.com/original/AST-0135469_ESG-Brief-HP-Maturity-Model-Oct-2014.pdf

Palermo, T. (2011) Research on Integrated Risk and Performance Management: the Time is Now, but How? *Risk & Regulation.* Centre for Analysis of Risk & Regulation (CARR), London: LSE

Palmer, R. (2011) *BCS Security Top Tips.* Security Community of Expertise (SCoE). March

Pappas, J.A. (2008) *A revitalized information assurance training approach and information assurance best practice rule set*, Doctoral dissertation, Monterey, California: Naval Postgraduate School

Parker, D.B. (1981) *Computer Security Management.* Reston: Prentice-Hall

Parker, D.B. (2010) Our Excessively Simplistic InfoSec Model and How to Fix It. *ISSA Journal*. July. **8**(7)

Parker, D.B. (2011) *Defining IA.* [email]. 22 February 2011. Personal communication to A. Simmons

Parker, D.B. (2015) Donn's Corner: Some advice for InfoSec Management. *ISSA Journal.* January. **13**(1), p.23

PCI Security Standards Council (SSC) (undated) *Payment Card Industry Data Security Standards (PCI DSS).* [online]. [Accessed 14 March 2016]. Available at: https://www.pcisecuritystandards.org/pci_security/

Peffers, K. (2007) A Design Science Research Methodology for IS. *Journal of Management Information Systems.* **24**(3). Winter 2007-8. pp.45-78. Chapter 2. In *Design Research in Information Systems: Theory and Practice.* Hevner & Chatterjee. 2010. Springer. [online]. [Accessed 3 May 2015]. Available at: http://www.springer.com/cda/content/document/cda_downloaddocument/9781441956521-c1.pdf?SGWID=0-0-45-929646-p173946050

Peltier, T.R. (2001) *InfoSec Risk Analysis*, Florida: CRC / Auerbach Publications

Peltier, T.R. (2002) *InfoSec Policies, Procedures, and Standards, Guidelines for Effective InfoSec Management.* Florida: CRC / Auerbach Publications

Peltier, T.R. (2004) *InfoSec Policies and Procedures, A Practitioner's Reference.* 2nd edition. p.3. Florida: CRC / Auerbach Publications

Peltier, T.R. (2005) Implementing an InfoSec Awareness Program. *InfoSec Today.* [online]. [Accessed 31 May 2015]. Available at: http://infosectoday.com/Articles/Peltier_awareness.pdf

Petersen, R. with Larsen, R., Schou, C. and Strickland, L. (2004) What's in a name? *EDUCAUSE Quarterly.* **27(**3), pp.5-8. [online]. [Accessed 13 May 2010]. Available at: http://www.educause.edu/EDUCAUSE+Quarterly/EDUCAUSEQuarterlyMagazineVolum/WhatsinaName/157298

Piatek, M. and Newkirk, J. (2009) Implementing IA – Beyond Process. In *The Interservice/ Industry Training, Simulation & Education Conference* (I/ITSEC). Volume **2009**. Metapress. [online]. [Accessed 3 February 2011]. Available at: http://ntsa.metapress.com/link.asp?id=r221638l6h4051r3

Ponemon, L. (2008) *Airport Insecurity: The Case of Lost Laptops*. Dell Corporation

Ponemon, L. (2010a) *Fourth Annual U.S. Cost of a Data Breach Study 2009.* PGP Corporation

Ponemon, L. (2010b) *First Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies.* Ponemon Institute LLC, ArcSight

Ponemon Institute LLC (2007) *2007 Annual Study: U.S. Cost of a Data Breach – Understanding Financial Impact, Customer Turnover, and Preventative Solutions.* PGP Corporation and Vontu, Inc.

Ponemon Institute LLC (2011) *Second Annual Cost of Cyber Crime Study: Benchmark Study of U.S. Companies*. Ponemon Institute LLC

Ponemon Institute (2012) *2011 Cost of Data Breach Study: Benchmark Study of U.S. Companies.* Ponemon Institute LLC

Ponemon Institute LLC (2013) *2013 Annual Cost of Failed Trust Report: Threats & Attacks*. Underwritten by Venafi

Ponemon Institute LLC (2014) *Exposing the Cybersecurity Cracks: A Global Perspective*, *Part 1: Deficient, Disconnected & in the Dark*. Websense Inc. [online]. [Accessed 26 April 2015]. Available at: https://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf

Ponemon Institute LLC (2014) *2014 Cost of Data Breach Study: Global Analysis*. [online]. [Accessed 2 March 2015]. Available at http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Pott, T. (2015) *I cannae dae it, cap'n! Why I had to quite the madness of frontline IT: With accountability comes decent budget*. The Register. [online]. 9 July. [Accessed 5 October 2015]. Available at: http://www.theregister.co.uk/2015/07/09/why_i_quit_it_sysadmin_overloads/?fb_action_ids=10153013216683354&fb_action_types=og.likes

Power, P. (2011) *Leaders – Legacies and Lessons:* Leading in a Crisis. *Continuity magazine.* [online]. pp.16-17. Picture used. [online]. [Accessed 15 March 2016]. Available at: http://image.slidesharecdn.com/previewoec-23leadershipmodels09-2014-141006060202-conversion-gate02/95/leadership-theories-by-operational-excellence-consulting-19-638.jpg?cb=1433773872

Poynter, K. (2008) *Review of InfoSec* at HMRC.[online]. [Accessed 7 February 2011]. Available at: http://webarchive.nationalarchives.gov.uk/+/http://www.hm-treasury.gov.uk/media/0/1/poynter_review250608.pdf

Prince, B. (2015) *Data Breach Costs Rise, Healthcare Industry Hardest Hit.* [online]. [Accessed 3 October 2015]. Available at: http://www.securityweek.com/data-breach-costs-rise-healthcare-industry-hardest-hit

Pugh, H. (2011) *IG: A Practical Approach for the Dodd-Frank Era.* [online]. [Accessed 18 February 2011]. Available at: http://www.wallstreetandtech.com/data-management/229216570

Quagliata, K. (2016) *The Role of the Adjunct in Educating the Security Practitioner.* In *ISSA Journal*. **14**(10), pp.26-30. October 2016

Quigley, M. (2008) *Encyclopedia of Information Ethics and Security.* Information Science Reference. New York: Hershey

Racz, N., Weippl, E. and Seufert, A. (2010) *A Frame of Reference for Research of Integrated GRC.* Bart Decker; Ingrid Schaumuller-Bichl. Communications and Multimedia Security, 6109, Springer. pp.106-117. Lecture Notes in Computer Science. [online]. [Accessed 31 August 2015]. Available at: https://hal.archives-ouvertes.fr/hal-01056386/document. Also available at: http://www.grc-resource.com/resources/racz_al_frame_reference_grc_cms2010.pdf

Raskin, V., Hempelmann, C. F., Triezenberg, K. E. and Nirenburg, S. (2001) *Ontology in InfoSec: a useful theoretical foundation and methodological tool.* In *Proceedings of the 2001 workshop on New Security Paradigms.* ACM. pp.53-59. [online]. [Accessed 20 September 2015]. Available at: http://dl.acm.org/citation.cfm?id=508180 also available at: http://dl.acm.org/citation.cfm?id=1628289

Ranum, M. (2005) The six dumbest ideas in computer security. *InfoSec Bulletin.* Volume **10**, pp.285–290

Rasmussen, M. (2015) From Backcountry Ranger to GRC Pundit. *LinkedIn Blog.* [online]. [Accessed 12 March 2015]. Available at: https://www.linkedin.com/pulse/from-backcountry-ranger-grc-pundit-michael-rasmussen?forceNoSplash=true

Rathmell, A. (2000) *Protecting Critical Information Infrastructures.* Compsec 2000 speech

Rathmell, A. (2001) *Building Partnerships to Protect Europe's Information Infrastructures.* ISSE presentation. [online]. Reference P-8063. California: RAND. [Accessed 14 March 2016]. Available at: http://www.rand.org/content/dam/rand/pubs/papers/2008/P8063.pdf

Rathmell, A. (2003) *Benchmarking IA in the Telecommunications Sector*

Raval, V. (2012) Changing Times and Eternality of Ethics. *ISACA Journal.* Volume **2**

Raval, V. (2016) Is IT Responsible for Corporate Crises. *ISACA Journal.* Volume **2**

Remenyi, D. (2014) *Grounded Theory: A Reader.* The Reader Series. 2nd edition. Reading: Academic Conferences Publishing International

Richardson, C.J. (2012) *Bridging the Air Gap: An IA Perspective.* PhD Thesis. University of Southampton

RIMS and IIA (2012) *Risk Management and Internal Audit: Forging a Collaborative Alliance.* [online]. [Accessed 12 July 2015]. Available at: https://global.theiia.org/standards-guidance/Public%20Documents/RIMS%20and%20The%20IIA%20Executive%20Report%20Forging%20a%20Collaborative%20Alliance.pdf

Rittel, H. W. and Webber, M. M. (1973) Dilemmas in a general theory of planning. *Policy Sciences.* [online]. **4**(2), pp.155-169. [Accessed 20 September 2015]. Available at: http://link.springer.com/article/10.1007/BF01405730#page-1

Room, S. (2009) *Butterworths Data Security Law & Practice.* Edinburgh: Lexis Nexis

Ross, S.J. (2013) Just Okay Practice. *ISACA Journal.* Volume **2**

SABSA (undated) *Sherwood Applied Business Security Architecture*. [online]. Accessed 7 September 2015]. Available at: http://www.sabsa.org/ and http://seccuris.abovesecurity.com/education-services/sabsa/

Saltzer, J. and Schroeder, M. (1975) The Protection of Information in Computer Systems. *Proceedings of the IEEE 63*. pp.1278-1308. [online]. [Accessed 6 June 2015]. Available at: https://www.cl.cam.ac.uk/teaching/1011/R01/75-protection.pdf

Schein, E.H. (1978) *Career Dynamics: Matching Individual and Organizational Needs.* Reading, MA: Addison-Wesley

Schlarman, S. (2015) *Announcing the RSA Archer Maturity Models.* [online]. [Accessed 21 September 2015]. Available at: https://community.emc.com/servlet/JiveServlet/showImage/38-11279-110038/ArcherMaturityModel.png

Schneier, B. (1999) *A plea for simplicity: You can't secure what you don't understand.* Schneier on Security. [online]. November. [Accessed 14 March 2016]. Available at: https://www.schneier.com/essays/archives/1999/11/a_plea_for_simplicit.html

Schneier, B. (2003) *Beyond Fear, Thinking Sensibly About Security in an Uncertain World.* New York: Copernicus Books

Schneier, B. (2015a) *Data and Goliath.* Cryptogram. [online].March. [Accessed 5 October 2015]. Available at: https://www.schneier.com/crypto-gram/archives/2015/0315.html#1

Schneier, B. (2015b) *Data and Goliath.*, New York: W.W. Norton & Company, Inc.

Schneier, B. (2017) *CSIS's Cybersecurity Agenda.* [online]. February. [Accessed 23 March 2017]. Available at: https://www.schneier.com/blog/archives/2017/02/csiss_cybersecu.html

Schou, C. and Shoemaker, D. (2007) *IA for the Enterprise: A Roadmap to InfoSec.* New York: McGraw-Hill Irwin

Schou, C.D. and Trimmer, K.J. (2004) IA and Security. *Journal of Organizational and End User Computing.* Idaho State University. **16**(3), p.1

Schwartz, M. (2015) Why data breach lawsuits fail: In most cases, proving 'injury' isn't easy. *Data Breach Today.* [online]. [Accessed 14 September 2015]. Available at: http://www.databreachtoday.com/so-many-data-breach-lawsuits-fail-a-8213

Scott, K. (2004) *An Analysis of Factors that have Influenced the Evolution of IA from World War I through Vietnam to the Present.* Thesis. AFIT/GIR/ENV/04M-22. Ohio: Air Force Institute of Technology

SC Magazine (2011) *Some things never change...*1969 *Management Today* article. Reprinted in full in *SC Magazine.* November-December. pp.26-30

Security Information Service for Business Overseas (2007) *China: Reducing Your Vulnerability to Commercial Espionage.* SISBO

Seddon, J. (2008) *Systems Thinking in the Public Sector: The failure of the reform regime…and a manifesto for a better way.* Axminster: Triarchy Press

Seldon, A. (2009) *Trust: How We Lost it and How to Get it Back*. UK: Biteback

Senge, P. (2000) *The leadership of profound change.* SPC Press. [online]. [Accessed 23 February 2011]. Available at: http://www.spcpress.com/pdf/Senge.pdf

Shah, S. (2013) Analysis: Recruiting an army of cyber guardians. *Computing.* [online]. 2 April. [Accessed 31 May 2015]. Available at: http://www.computing.co.uk/ctg/analysis/2257252/analysis-recruiting-an-army-of-cyber-guardians

Shanes, P. and Ciechanowicz C. (2011) *Accreditation: An end-to-end approach to managing IA within the MoD.* [online]. Technical Report, Royal Holloway Series of articles, 8 March. [Accessed 31 May 2015]. Available at: https://www.ma.rhul.ac.uk/static/techrep/2011/RHUL-MA-2011-08.pdf

Shannon, C.E. (1948) *A Mathematical Theory of Communication.* [online]. [Accessed 14 March 2016]. Available at: http://seclab.cs.ucdavis.edu/projects/history/seminal.html

Sherwood, J., Clark, A. and Lynas, D. (2005) *Enterprise Security Architecture, A Business-Driven Approach*. San Francisco: CMP Books

Shostack, A. and Stewart, A. (2008) *New School of InfoSec.* Boston: Addison Wesley

Silverman, D. (2009) *Interpreting Qualitative Data*. 3rd edition. London: Sage Publishing

Simmons, A.C. (2009) *Achieving Best Practice in Public Sector InfoSec.* London: Ark Group

Simmons, A.C. (2010) *Tackling the barriers to achieving best practice in IA in the UK Public Sector.* [online]. Oxford: ARCS Workshop

Simmons, A.C. (2011) MSc proposed course structure [Available at: **Appendix 1: Section 10.3**]

Simmons, A.C. (2012a) *Once more unto the breach: – Managing InfoSec in an Uncertain World.* IT Governance

Simmons, A.C. (2012b) Understanding Control Standards within the Context of Standards. Compliance and Governance. *ISSA Journal.* **10**(8), pp.24-29

Simmons, A.C. (2015a) *Once more unto the Breach: Managing InfoSec in an uncertain world.* 2nd edition. Cambridge: IT Governance Publishing

Simmons, A.C. (2015b) IA: Adapting to New Metaphors. *ISSA Journal.* **13**(9), pp.16-26

Simms, J. (2011) In plain English, please. *Director magazine.* p.26

Smith, T. (undated) *You can't improve what you Don't Measure.* [online]. [Accessed 18 March 2016]. Available at: http://www.littlethingsmatter.com/blog/2010/08/23/you-cant-improve-what-you-dont-measure/

Socitm Insight (2004b) *Knock, knock: who's there? An overview of authentication for electronic service delivery.* Executive briefing

SOLACE (2000) *Chance or Choice? Risk Management and Internal Control guidance for Local Government with SOLACE and Zurich Municipal Management Services* (ZMMS). [online]. [Accessed 8 February 2011]. Available at: http://www.emeraldinsight.com/journals.htm?articleid=868041&show=html

Spada (2009) *British Professions Today: The State of the Sector*, Spada Limited

Spafford, E. (2001) *IA and Security, House of Representatives Science Committee.* Statement. [online]. [Accessed 14 March 2016]. Available at: http://spaf.cerias.purdue.edu/usgov/house01.pdf

Spender, J.-C. (1996) Making knowledge the basis of a dynamic theory of the firm. *Strategic Management Journal.* Wiley. **17**(S2), pp.45-62

Spice, B. (2007) *The death of computer science is greatly exaggerated – again.* News blog. [online]. [Accessed 2 October 2015]. [No longer available]

Stahl, B.C. (2004) Responsibility for IA and Privacy: A Problem of Individual Ethics? *Journal of Organizational and End User Computing.* Jul-Sep. **16**(3), p.59. ABI/INFORM Global

Stamper, R. (1973) *Information in Business and Administrative Systems.* London: Batsford

Stanford, M. (1986) *The Nature of Historical Knowledge.* Oxford: Blackwell

Stein, G. (2010) *Managing People and Organizations: Peter Drucker's Legacy.* Bingley: Emerald Group Publishing Limited

Stevens, T. (2009) Question the assumptions. *GC Magazine*

Stewart, G. (2014) Say What You Mean. *ISSA Journal.* **12**(11), p.8

Stewart, G. (2015) Keeping It Simple. *ISSA Journal.* **13**(1), p.7

Straub, D.W., Gefen, D. and Boudreau, M.C. (2005) *Quantitative Research.* In Avison, D. and Pries-Heje, J. (eds.) *Research in IS: A Handbook for Research Supervisors and Their Students*. Amsterdam: Elsevier, pp.221–238

Sundt, C. (2002) *InfoSec Consultancy: A Study for The DTI*

Susman, G.I. and Evered, R.D. (1978) An Assessment of the Scientific Merits of Action Research. *Administrative Science Quarterly.* pp.582-603

Switzer, C. (2011) GRC background explanation. [email], personal comms from Carole Stern Switzer, Esq. President to A. Simmons. Open Compliance & Ethics Group (OCEG)

Tawileh, A. and McIntosh, S. (2007) *Understanding IA: A Soft Systems Approach.* School of Computer Science. Cardiff University. [online]. [Accessed 14 September 2015]. Available at: http://www.tawileh.net/anas//files/downloads/papers/InfoAssurance-SSM.pdf?download

Taylor, A., Alexander, D., Finch, A. and Sutton, D. (2008) *InfoSec Management Principles, An ISEB Certificate.* Swindon: BCS Publishing

Taylor Baines (2013) *The Internal Audit Review.* [online]. [Accessed 15 March 2016]. Available at: http://www.taylorbaines.co.uk/resources/Assurance%20Model.png

The World Bank (2004) *Technology Risk Checklist.* Version 7.3. World Bank Integrator Unit and TRE Security Team Collaboration

Thomas, R. and Walport, M. (2008) *Data Sharing Review Report.* [online]. [Accessed 7 February 2011]. Available at: http://www.justice.gov.uk/reviews/datasharing-intro.htm

Thomson Reuters (2013a) *Risk Culture and Conduct Control: Time for a more enlightened approach.* Accelus. Dr Roger Miles

Tibbs, H., Ambler-Edwards, S. and Corcoran, M. (2013) *The Global Cyber Game: Achieving Strategic Resilience in the Global Knowledge Society,* Defence Academy of The United Kingdom: Shrivenham. [online]. [Accessed 13 March 2016]. Available at: http://www.futurelens.com/wp-content/uploads/2014/04/The-Global-Cyber-Game.pdf

Timberg, C. (2015) *A disaster foretold, and ignored.* Washington Post. [online]. [Accessed 3 October 2015]. Available at: http://www.washingtonpost.com/sf/business/2015/06/22/net-of-insecurity-part-3/

Toffler, A. (1970) *Future Shock.* Random House, Bantam Books. (Reprinted 1981)

Toomey, M. (2011) *The Infonomics Letter, Plain Language about Leadership and (Corporate) Governance of IT.* March and June editions. [online]. [Accessed 23 March 2016]. Available at: http://www.infonomics.com.au/Newsletter.htm

TopGear (2016) *Emissions scandal latest: Mitsubishi admits cheating since 1991.* [online]. 26 April 2016. [Accessed 2 May 2016]. Available at: http://www.topgear.com/car-news/insider/emissions-scandal-latest-mitsubishi-admits-cheating-1991

Tsoumas, B. (2006) *On the basis of an assurance by ontology paradigm proposal*, NATO ARW on InfoSec: Assurance and Security

Turnbull, S. (2002) *A New Way to Govern: Organisations and Society After Enron*. New Economics Foundation Pocketbook 6. [online]. [Accessed 15 February 2011]. Available at: http://ssrn.com/abstract=319867 or doi:10.2139/ssrn.319867

Tranfield, D. and Braganza, A. (2007) *Business Leadership of Technological Change: Five Key Challenges Facing CEOs.* London: Chartered Management Institute

Translink (2009) *Purchase of IT, Systems and Equipment TPP125*. [online]. [Accessed 14 March 2016]. Available at: http://www.niassembly.gov.uk/globalassets/documents/raise/deposited-papers/2015/dp1450_29.pdf

Trim, P.R.J. and Caravelli, J. (2009) *Strategizing Resilience and Reducing Vulnerability.* New York: Nova Science Publishers, Inc.

Tyrrell, I. and Seddon, J. (2014) How bureaucrats destroy public services, and what can be done about it. Conversations, in *Human Givens Journal.* **21**(2), pp.28-33

UNC Charlotte (2015) *IA is a Shared Responsibility*. [online]. [Accessed 15 March 2016]. Available at: http://itservices.uncc.edu/home/information-security/information-assurance

UK Cabinet Office (1999a) *Modernising Government White Paper.* [online]. [Accessed 3 February 2011]. Available at: http://www.nationalschool.gov.uk/policyhub/docs/modgov.pdf

UK Cabinet Office (2002a) *Security: e-Government Strategy Framework Policy and Guidelines,* Version 4.0

UK Cabinet Office (2002b) e-*GIF Registration & Authentication framework*

UK Cabinet Office (2004a) *Protecting our information systems: Working in partnership for a secure and resilient UK information infrastructure*. CSIA. 262949/0604/D40

UK Cabinet Office (2005c) *Transformational Government: Enabled by Technology*

UK Cabinet Office (2007a) *A National IA Strategy.* CSIA

UK Cabinet Office (2007c) *Delivering the IA Strategy.* CSIA. Version 1.10

UK Cabinet Office (2007d) *Data Handling Procedures in Government: Interim Progress Report.* Robert Hannigan. [online]. [Accessed 3 February 2011]. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/data_handling-interim.pdf

UK Cabinet Office (2008a) *Data Handling Procedures in Government.* [online]. [Accessed 2 September 2015]. Available at: http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

UK Cabinet Office (2008b) *Final report on Data Handling Procedures across government.* [online]. [Accessed 2 September 2011]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60966/final-report.pdf

UK Cabinet Office (2008d) *Cross Government Actions: mandatory minimum measures.* [online]. [Accessed 3 February 2011]. Available at: http://www.cabinetoffice.gov.uk/sites/default/files/resources/cross-gov-actions.pdf

UK Cabinet Office (2009a) *Power of information Task Force Report 2009.* [online]. [Accessed 2 September 2015]. Available at: https://powerofinformation.wordpress.com/2009/03/04/final-report/

UK Cabinet Office (2009b) *Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space.* CM7642. London: HMSO. [online]. [Accessed 27 March 2011]. Available at: www.cabinetoffice.gov.uk/media/216620/css0906.pdf

UK Cabinet Office (2009c) *Power in People's Hands: Learning from the World's Best Public Services.* Ref: 296673 / 0709. [online]. [Accessed 6 February 2011]. Available at: http://www.eduweb.vic.gov.au/edulibrary/public/teachlearn/innovation/panddc/Power_in_Peoples_Hands.pdf

UK Cabinet Office (2009d) *HMG IA Maturity Model and Assessment Framework.* Version 3.0. Updated Version 4.0

UK Cabinet Office (2009e) *Government ICT Strategy: New World, New Challenges, New Opportunities*

UK Cabinet Office (2009f) *HMG Security Policy Framework.* V3.0. ***Updated 2014***. [online]. [Accessed 21 September 2015]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

UK Cabinet Office (2009g) *HMG Security Policy Framework, Roles and Responsibilities*. V3.1

UK Cabinet Office (2010a) *Protecting Information in Government*. [online]. [Accessed 31 May 2015]. Available at: http://systems.hscic.gov.uk/infogov/links/caboffprotectinfo.pdf

UK Cabinet Office (2010b) *Government ICT strategy: smarter, cheaper, greener.* London: HMSO. [online]. [Accessed 27 March 2011]. Available at: http://www.epractice.eu/files/Government%20ICT%20Strategy%20-%20Smarter,%20cheaper,%20greener.pdf

UK Cabinet Office (2011a) *Data Centre Strategy, G-Cloud & Government Applications Store Programme Phase 2.* Scope Report. Version No. 0.35

UK Cabinet Office (2011b) *PSN Technical Transition Guidance.* Version No. 08. [online]. [Accessed 23 March 2016]. Available at: https://www.gov.uk/government/groups/public-services-network

UK Cabinet Office (2011c) *Government ICT Strategy.* London: Whitehall

UK Cabinet Office (2011d) *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world.* Ref: 407494/1111. [online]. [Accessed 3 May 2015]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf

UK Cabinet Office (2011e) *Corporate governance in central government departments: Code of good practice 2011.* With HM Treasury. London: Whitehall

UK Cabinet Office (2013a) *Government Security Classifications.* Version 1.0. [online]. [Accessed 15 March 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/251480/Government-Security-Classifications-April-2014.pdf

UK Cabinet Office (2013b) *Cyber governance health check.* [online]. [Accessed 15 March 2016]. Available at: https://www.gov.uk/government/publications/cyber-governance-health-check

UK Central Sponsor for Information Assurance (CSIA) (2002) *Introductory presentation to IAAC*

UK CSIA (2003) *A United Kingdom Government Strategy for IA.* Draft Version 0.3

UK CSIA (2008) *Data Handling Review engagement with industry* (papers, panellist member)

UK Centre for Protection of National Infrastructure (CPNI) (2010) *Sources of Guidance on Security in the Telecommunications Sector.* [Accessed 5 February 2011]. [No *longer available, 15 March 2016]*

UK CPNI (2012) *Top 20 Critical Controls for Effective Cyber Defence*

UK CESG (undated) *Certification.* Cheltenham: CESG. [online]. [Accessed 20 March 2011]. Available at: http://www.cesg.gov.uk/products_services/iacs/cc_and_itsec/media/intro-guides/cccert.pdf

UK CESG (2009e) *HMG IA Standard No.6 - Protecting Personal Data and Managing Information Risk* (originally known as the Minimum Mandatory Requirements). Issue 1.2. Cheltenham: CESG

UK CESG (2009f) *HMG IA Standard No. 1, Technical Risk Assessment.* Issue No: 3.51. Cheltenham: CESG – see http://en.wikipedia.org/wiki/HMG_Infosec_Standard_No.1. [online]. Accessed 1 March 2015]. Available at http://www.cesg.gov.uk/publications/Documents/is1_risk_assessment.pdf,

UK CESG (2009g) *HMG IA Standard 4 – Communications Security and Cryptography.* Issue 4.0

UK CESG (2009h) *HMG IA Standard 5 - Secure Sanitisation of Protectively Marked or Sensitive Information.* Issue 3.1

UK CESG (2010a) *HMG IA Standard 2 – Risk Management and accreditation of systems.* Issue 3.2. Cheltenham: CESG

UK CESG (2010c) *Busy Reader Guide – Improving IA at the Enterprise Level.* Issue No. 1.0. Cheltenham: CESG

UK CESG (2010d) *Busy Reader Guide - Requirements for Secure Delivery of Online Public Services.* Issue No: 1.0. Cheltenham: CESG

UK CESG (2010e) *Miscellaneous - Requirements for Secure Delivery of Online Public Services Part 1 – Principles.* Issue No: 1.0. Cheltenham: CESG

UK CESG (2010f) *Miscellaneous - Requirements for Secure Delivery of Online Public Services - Part 2 - Security Components.* Issue No: 1.0. Cheltenham: CESG

UK CESG (2010g) *Tailored Assurance Services* (CTAS). Cheltenham: CESG. [online]. Available at: http://www.cesg.gov.uk/products_services/iacs/ctas/index.shtml

UK CESG (2010h) *What is IA?* Cheltenham: CESG. [online]. [Accessed 7 February 2011]. Available at: http://www.cesg.gov.uk/about_us/whatisia.shtml

UK CESG (2010i) *HMG IA Maturity Model (IAMM) and Assessment Framework.* Version 4.0. Cheltenham: CESG. [online]. Available at: http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

UK CESG (2011) *Supplier IA Assessment Framework and Guidance.* Issue 1.0. [online]. Available at: http://www.cesg.gov.uk/publications/media/policy/supplier_ia_assessment_framework.pdf

UK CESG (2012a) *Cyber Security Guidance for Business.* [online]. [Accessed 15 March 2016]. Available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

UK CESG (2012b) *Requirements for Secure Delivery of Online Public Services – Annex B: Security Components.* Good Practice Guide (GPG) No. 43. Issue No 1.1. [online] [Accessed 1 March 2015]. Available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/270970/GPG_43_RSDOPS_Annex_B_issue_1.1_Dec_2012.pdf

UK CESG (2013) *IAMM Self-Assessment Guide.* [online]. 18 February. Version 1.2. p.9. [Accessed 15 March 2016]. Available at: https://www.cesg.gov.uk/articles/ia-maturity-model-self-assessment-and-supported-self-assessment

UK Department for Business Enterprise & Regulatory Reform (BERR) (2008) *Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing*

UK Department for Culture Media and Sport (DCMS) and Department for Business, Innovation & Skills (BIS) (2009) *Digital Britain Report.* [online]. [Accessed 3 April 2014]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228844/7650.pdf

UK Department of Trade and Industry (DTI) (1996) *Protecting business information: Keeping it confidential.* London: DTI InfoSec Policy Group

UK DTI (1999) *Building confidence in Electronic Commerce – A Consultation Document.* URN 99/642. [online]. [Accessed 14 March 2016]. Available at: http://www.cyber-rights.org/crypto/consfn1.pdf

UK DTI (2002) *DTI InfoSec Breaches Survey 2002.* Technical Report. PricewaterhouseCoopers

UK GCHQ (2015) *10 Steps to Cyber Security.* Including *10 Steps: Summary.* [online] [Accessed 2 December 2015]. Available at: http://www.gchq.gov.uk/press_and_media/news_and_features/Pages/Relaunch-10-Steps-to-Cyber-Security.aspx Various supporting publications are available at: https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

UK Government Office for Science (2009) *Cyber Trust and Crime Prevention Mid-Term Review.* [online]. November 2005 – January 2009. Foresight. [Accessed 17 May 2015]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/299216/04-1137-cyber-trust.pdf

UK Government Office for Science (2014) *The Internet of Things: making the most of the Second Digital Revolution: A Report by the UK Government Chief Scientific Adviser.* [online]. Mark Walport. URN: GS/14/1230. [Accessed 11 September 2015]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/409774/14-1230-internet-of-things-review.pdf

UK HMG (2003a) *Foresight Cyber Trust and Crime Prevention Programme (CTCP)*

UK HMG (2003b) *HMG Minimum Requirements for the Verification of the Identity of Organisations V2*

UK HMG (2003c) *HMG Minimum Requirements for the Verification of the Identity of Individuals V2.* [Accessed 1 March 2015]. [No longer available online]

UK HMG (2008a) *Managing Information Risk, A guide for Accounting Officers, Board members and Senior Information Risk Owners*

UK HMG (2008b) *Information matters: building government's capability in managing knowledge and information.* Knowledge Council. [online]. [Accessed 13 November 2010]. Available at: http://gkimn.nationalarchives.gov.uk/gov-strategy.htm

UK HMG (2011b) *Fighting Fraud Together: The strategic plan to reduce fraud.* [online]. [Accessed 13 July 2015]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118501/fighting-fraud-together.pdf

UK HMG (2014) *Cyber Essentials Scheme*. [online]. [Accessed 15 March 2016]. Available at: http://cyberessentialsscheme.com/ and https://www.cyberstreetwise.com/cyberessentials/

UK HMG (2016a) *Prospectus: Introducing the National Cyber Security Centre*. May 2016. [online]. [Accessed 10 October 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf

UK HMG (2016b) *National Cyber Security Strategy 2016 – 2021.* November 2016. [online]. [Accessed 4 November 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/564268/national_cyber_security_strategy.pdf

UK HM Treasury (2004) *The Orange Book: Management of Risk – Principles and Concepts*, ISBN 1-84532-044-1-1. [online]. [Accessed 9 September 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/220647/orange_book.pdf

UK HM Treasury (2006) Thinking about risk: Managing your risk appetite: A practitioner's guide, November 2006, ISBN 1-84532-232-0

UK Home Office (2010) *Cyber Crime Strategy.* Cm 7842. London: HMSO. [online]. [Accessed 6 March 2011]. Available at: http://www.official-documents.gov.uk/document/cm78/7842/7842.pdf

UK House of Commons Committee of Public Accounts (2017) *Protecting information across government.* Thirty-eighth Report of Session 2016-2017. 25 January 2017. HC769

UK House of Commons Home Affairs Committee (2008) *A Surveillance Society?* Fifth Report of Session 2007–08. Volume **I**. [online]. [Accessed 7 February 2011]. Available at: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmhaff/58/58i.pdf

UK House of Commons Defence Committee (2002) *Defence and Security in the UK, Sixth Report of Session 2001-02. HC518-1.* London: HMSO The Stationary Office. [online]. [Accessed 15 March 2016]. Available at: http://www.parliament.the-stationery-office.co.uk/pa/cm200203/cmselect/cmdfence/93/9304.htm

UK House of Commons Justice Committee (2008) *Protection of Private Data Report.* [online]. [Accessed 7 February 2011]. Available at: http://www.publications.parliament.uk/pa/cm200708/cmselect/cmjust/154/154.pdf

UK Information Commissioner's Office (ICO) (2006) *A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network* [online]. Full Report. [Accessed 6 February 2011]. Available at: www.ico.gov.uk/upload/documents/library/data_protection/practical_application/surveillance_society_full_report_2006.pdf. [Accessed 1 March 2015]. Summary available at: https://ico.org.uk/media/about-the-ico/documents/1042391/surveillance-society-summary-06.pdf

UK ICO (2008a) *Taking Stock, Taking Action: The ICO position on the Government Data Handling Reviews.* Cheshire: ICO

UK ICO (2008b) *Privacy by Design report*

UK ICO (2009) *Privacy Impact Assessment Handbook*

UK ICO (2015) *ICO response to ECJ ruling on personal data to US Safe Harbor.* Statement. [online]. [Accessed 23 March 2016]. Available at: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2015/10/ico-response-to-ecj-ruling-on-personal-data-to-us-safe-harbor/

UK KTN (2015) *Draft Horizon 2020 work Programme 2016-2017 in the area of Secure societies – Protecting freedom and security of Europe and its citizens.* [online]. [Accessed 26 September 2015]. Available at: https://ec.europa.eu/programmes/horizon2020/sites/horizon2020/files/14.%20Secure%20societies_2016-2017_pre-publication.pdf

UK Ministry of Defence (MoD) (2008) *MOD Action Plan in response to Burton Report.* [online]. [Accessed 7 February 2011]. Available at: http://www.mod.uk/NR/rdonlyres/F0437ECE-F5E6-4246-B4A8-8E63B789C915/0/burton_action_plan20080625.pdf. See also: http://www.mod.uk/DefenceInternet/AboutDefence/CorporatePublications/PolicyStrategyandPlanning/ReportIntoTheLossOfModPersonalData.htm

UK MoD (2013) *Cyber Primer.* [online]. [Accessed 13 March 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/360973/20140716_DCDC_Cyber_Primer_Internet_Secured.pdf

UK NHS (2015) *NHS IG Toolkit* [online]. [Accessed 2 February 2015]. Available at: https://www.igt.hscic.gov.uk/ and https://www.igt.hscic.gov.uk/resources/About%20the%20IG%20Toolkit.pdf

UK Office of the Deputy Prime Minister (ODPM) (2002) *The National Strategy for local e-government*

UK ODPM (2003) *One Year On, The National Strategy for local e-government*

UK ODPM (2004a) *Doing Business Electronically – Delivering e-Procurement, Guidance Summary & Index to Web Materials*

UK ODPM (2004b) *The Benefits of e-Procurement*

UK ODPM (2004c) *Working with Business, Your business made easy – Survey of English local authority websites from a business perspective*

UK ODPM (2004d) *National Projects at the heart of excellent services, Benefits Guides – Executive Summary*

UK ODPM (2004e) *National e-Procurement Project, Delivering e-Procurement, 2004 Survey Results*

UK Office of the e-Envoy (OeE) (2002a) *In the service of democracy, a consultation paper on a policy for electronic democracy*

UK OeE (2002b) *Open Source Software use within UK Government.* [online]. [Accessed 14 March 2016]. Available at: http://xml.coverpages.org/UK-ossPolicydocument20020715.pdf

UK OeE (2002c*) e-Government Strategy Framework Policy and Guidelines.* Version 4.0

UK OeE (2002d) *e-Government strategy framework policy and guidelines, business services.* Version 2.0

UK OeE (2002e) *e-Government strategy framework policy and guidelines, confidentiality.* Version 3.0

UK OeE (2002f) *e-Government strategy framework policy and guidelines, network defence.* Version 2.0

UK OeE (2002g) *e-Government strategy framework policy and guidelines, registration and authentication.* Version 3.0

UK OeE (2002h) *e-Government strategy framework policy and guidelines, security architecture.* Version 2.0

UK OeE (2002g) *e-Government strategy framework policy and guidelines, trust services.* Version 3.0

UK OeE (2002h*) e-Government strategy framework policy and guidelines, assurance*

UK OeE (2002k) *e-Government strategy framework policy and guidelines, IA & Corporate Governance - What every director must know.* Version 4.0

UK Online (2000) *A BBC report referring to the programme.* [online]. [Accessed 6 March 2011]. Available at http://news.bbc.co.uk/1/hi/uk_politics/919903.stm

UK Parliamentary Office of Science and Technology (POST) (2006a) *Postnote, Pervasive Computing.* No 263

UK POST (2006b) *Postnote, Data Encryption*. No 270

UK POST (2006c) *Postnote, Computer Crime*. No 271

UK POST (2007a) *Postnote, Internet Governance*. No 279

UK POST (2007b) *Postnote, Grids and e-Science*. No 286

UK Public Administration Select Committee (2010) *The Commons PASC Good Governance – the effective use of IT*

Uschold, M. and King, M. (1995) *Towards a Methodology for Building Ontologies.*, AIAI-TR-183. Presented at *Workshop on Basic Ontological Issues in Knowledge Sharing* held in conjunction with IJCAI-95. University of Edinburgh, UK. [online]. [Accessed 24 June 2015]. Available at: http://www1.cs.unicam.it/insegnamenti/reti_2008/Readings/Uschold95.pdf

US CNSS (2003) *Committee on National Security Systems Instruction 4009 National IA Glossary,* formerly NSTISSI 4009 (National Security Telecommunications and Information Systems Security Committee), original May 2003, updated 26 April 2010. [online]. [Accessed 2nd February 2011]. Available at http://www.pdfchaser.com/CNSS-RM-Policy-and-Framework.html

US Department of the Air Force (2001) AFI33-204: *IA Awareness Program.* [online]. [Accessed 2 February 2011]. Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA405017

US Department of Defense (DoD) (1998) *Joint Doctrine for Information Operations.* Joint Publication 3-13. Joint Chiefs of Staff. 9 October . Updated 27 November 2012 and 20

November 2014. [online]. [Accessed 13 September 2015]. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf

US DoD (2017) *DoD Cybersecurity Policy Chart.* [Previously the *IA Policy Chart*] Last updated 30 June 2017. [online]. [Accessed 17 July 2017]. Available at: http://iac.dtic.mil/csiac/download/ia_policychart.pdf

US Department of Homeland Security (DHS) (2003) *National Strategy to Secure Cyberspace.* [online]. [Accessed 15 March 2016]. Available at: https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf

US DHS (2008) *Information Technology (IT) Security Essential Body of Knowledge (EBK): A Competency and Functional Framework for IT Security Workforce Development*. [online]. [Last accessed 4 February 2018]. Available at: http://trygstad.rice.iit.edu:8000/Books/ITSecurityEssentialBodyOfKnowledge2008-USDeptOfHomelandSecurity.pdf

US DHS (2010) *Software Assurance Universe.* [online]. [Accessed 12 April 2011]. Available at: https://buildsecurityin.us-cert.gov/swa/procwg.html and https://buildsecurityin.us-cert.gov/swa/index.html

US DHS (2014) *The Path towards Cybersecurity Professionalization: Insights from Other Occupations.* Version 2.0. [online]. [Accessed 6 October 2014]. Available at: http://niccs.us-cert.gov/sites/default/files/documents/files/The%20Path%20Towards%20Cybersecurity%20Professionalization_0.pdf

US National Institute of Standards and Technology (NIST) (1995) *NIST SP 800-12: An Introduction to Computer Security: The NIST Handbook*

US NIST (2001b) *NIST SP 800-33: Underlying Technical Models for ITSec.* [online]. [Accessed 6 February 2011]. Available at: http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf

US NIST (2004a) *FIPS PUB 199 Standards for Security Categorization of Federal Information and Information Systems*

US NIST (2015) *CPS PWG Draft CPS Framework*

US NSTISSI (1994) *NSTISSI No. 4011: National Training Standard for IS Security (InfoSec) Professionals*

US NSTISSI (2000) *NSTISSI No.1000: National IA Certification and Accreditation Process (NIACAP)*

US NSTISSP (2003) *NSTISSP No. 11: Revised Fact Sheet, National Assurance Information Acquisition Policy*

Vaas, L. (2015) Microsoft age-guessing tool goes on a metadata-slurping, viral spree, *Sophos Naked Security newsletter.* [online]. 1 May. [Accessed 4 May 2015]. Available at: https://nakedsecurity.sophos.com/2015/05/01/microsoft-age-guessing-tool-goes-on-a-metadata-slurping-viral-spree/

Vaidya, T. (2015) *2001-2013: Survey and Analysis of Major Cyberattacks.* Preprint arXiv:1507.06673. Georgetown University. [online]. [Accessed 17 March 2016]. Available at: http://arxiv.org/pdf/1507.06673.pdf

Valentine, E. (2015) *Enterprise Business Technology Governance: new core competencies for boards of directors in digital leadership*. Thesis. Australia: Queensland University of Technology, Brisbane

Valsmith (2015) *Hard to sprint when you have two broken legs.* CarnalOwnage blog. [online]. June. [Accessed 13 September 2015]. Available at: http://carnal0wnage.attackresearch.com/2015/06/hard-to-sprint-when-you-have-two-broken.html

Vanguard Consulting Limited (2001) *The Vanguard Guide to Your Organisation as a System*, edited by Bryce Harrison Inc.

Varney, D. (2006) *Service transformation: A better service for citizens and businesses, a better deal for the taxpayer.* [online]. [Accessed 15 March 2016]. Available at:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/229012/011840489X.pdf

Verizon (2009) *Data Breach Investigations Report*. [online]. [Accessed 23 March 2016]. Available at: http://www.verizonbusiness.com/resources/security/reports/2009_databreach_rp.pdf

Verizon (2010) *Data Breach Investigations Report.* [online]. [Accessed 20 April 2011]. Available at: http://www.verizonbusiness.com/resources/reports/rp_2010-data-breach-report_en_xg.pdf plus Exec Summary available at: http://www.verizonenterprise.com/resources/executivesummaries/es_2010-data-breach-report_en_xg.pdf

Verizon (2011) *Data Breach Investigations Report.* [online]. [Accessed 20 April 2011]. Available at: http://www.verizonbusiness.com/go/2011dbir

Verizon (2012) *Data Breach Investigations Report.* [online]. [Accessed 13 March 2016]. Available at: http://www.wired.com/images_blogs/threatlevel/2012/03/Verizon-Data-Breach-Report-2012.pdf

Verizon (2015) *2015 Data Breach Investigation Report (DBIR).* WP16368 4/15. [online]. [Accessed 25 April 2015]. Available at: http://www.verizonenterprise.com/DBIR/2015/

Verizon (2017) *2017 Data Breach Investigation Report (DBIR).* WP16368 4/15. [online]. [Accessed 4 May 2017]. Available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

Vicente, P.F.O. (2011) *A Reference Architecture for Integrated Governance Risk and Compliance.* Lisbon University. Thesis. [online]. [Accessed 2 May 2015]. Available at: https://fenix.tecnico.ulisboa.pt/downloadFile/395143146329/disserta%C3%A7%C3%A3o.pdf

Vijayan, J. (2015) *Security Spending and Preparedness in the Financial Sector: A SANS Survey.* [online]. [Accessed 7 March 2015]. Available at: https://www.sans.org/reading-room/whitepapers/analyst/security-spending-preparedness-financial-sector-survey-36032

Vinson, N.G. and Singer, J. (2001) *Getting to the Source of Ethical Issues.* Empirical Software Engineering. **6**(4), pp.293–297

Virgo, P. (2011) Why do we never learn? The pre-conditions for public sector systems success. *Computer Weekly.* [online].1 November. [Accessed 21 January 2011]. Available at: http://www.computerweekly.com/blogs/when-it-meets-politics/2011/01/why-do-we-never-learn-the-pre-.html?cp=NLC-CWNEW20110119&attr=headlines

Virgo, P. (2014) *Draft Interim Report (Version 4.1) on engaging financial services employers with the Cyber Security Apprenticeship and CPD frameworks and programmes being developed by e-Skills and its partners.* 21 July

Viscarolasaga, E. (2009) Ethical Choices. *InfoSecurity Professional.* **3**(7), p.11

Von Solms, B. (2001) *InfoSec - a multidimensional discipline.* In Computers & Security. **20**(6). Elsevier, pp.504-508

Wadsworth, Y. (1998) *What is Participatory Action Research?* [online]. Action Research International Paper 2. [Accessed 6 June 2011]. Available at http://www.scu.edu.au/schools/gcm/ar/ari/p-ywadsworth98.html

Walters, R. (2011) Governance: Fleshing Out the Framework. *ISSA Journal.* **9**(2)

Warren, M. (2016) *Professional identities and regulation: a Literature Review,* Professional Standards Authority, December 2016

Watzlawick, P. (1978) *The Language of Change*. New York: Basic Books

Weill, P. and Ross, J. (2005) *A Matrixed Approach to Designing IT governance.* MIT Sloan Management Review. **46**(2). Winter

Whittaker, Z. (2015) *This is the worst password from the Ashley Madison hack.* [online]. ZDNet. 5 September. [Accessed 4 October 2015]. Available at: http://www.zdnet.com/article/these-are-the-worst-passwords-from-the-ashley-madison-hack/

Wilcox, J. (2005) Developing professional skills. *UK Centre for Materials Education*. [Accessed 12 March 2017]. Available at: https://www.researchgate.net/profile/Colin_Coles/publication/9023041_Developing_professional_skills/links/561f6dd908aec7945a28153f.pdf

Williams, P.D. (2008) *Security studies: an introduction*. Oxfordshire: Routledge. ISBN: 0-203-92660-9

Williams, R. (2014) Anti-Intellectualism and the "Dumbing Down" of America: There is a growing anti-intellectual dumbing down of our culture. *Psychology Today.* [online]. [Accessed 12 March 2016]. Available at: https://www.psychologytoday.com/blog/wired-success/201407/anti-intellectualism-and-the-dumbing-down-america

Willetts, K. (2008) *IA Architecture.* Florida: Auerbach Publications/CRC Press

Wolff, J. (2014) Cybersecurity as Metaphor: Policy and Defense Implications of Computer Security Metaphors (March 31, 2014). 2014 TPRC Conference Paper. [online]. [Accessed 2 May 2017]. Available at SSRN: http://dx.doi.org/10.2139/ssrn.2418638 or https://ssrn.com/abstract=2418638

Wooding, S., Anhal, A. and Valeri, L. (2003) *Raising Citizen Awareness of InfoSec: A Practical Guide.* [online]. [Accessed 15 March 2016]. Available at: https://www.clusit.it/whitepapers/eaware_practical_guide.pdf

World Economic Forum (2012) *Insight Report: Risk and Responsibility in a Hyperconnected World*, *Pathways to Global Cyber Resilience.* p.13. [online]. [Accessed 13 September 2015]. Available at: http://www3.weforum.org/docs/WEF_IT_PathwaysToGlobalCyberResilience_Report_2012.pdf

Wright, A. (2011) *"Not on my watch" Enterprise Governance Risk & Compliance …and how to survive it.* Adrian Wright, CEO - Secoda Risk Management Director of Projects - ISSA-UK. White-hats meeting 2nd December. London: IoD

Wright, P. (2008a) *Hi-Tech Crime Strategy and Budget for 2011*

Wright, P. (2008b) *Hi-Tech Investigative Research, The illicit trade in Pharmaceuticals*

Wright, P. (2008c) *Insecure Internet Access via wireless*

Wylder, J. (2004) *Strategic InfoSec.* Florida: CRC / Auerbach Publications, p.21/p.28

YAS (2011) *Yorkshire Ambulance Service IG* web pages. [online]. [Accessed 23 March 2016]. Available at: http://www.yas.nhs.uk/InformationGovernance/Information%20Governance.html

Young, R. (2008) *What is meant by reflexivity in the context of ethnographic research? Does reflexivity have limits?* Essex University. [online]. [Accessed 5 June 2011]. Available at www.essex.ac.uk/sociology/.../**RebeccaYoung**_SC203_2008.pdf

Zorabedian, J. (2015) *TalkTalk breach: CEO dismisses encryption, 15-year-old arrested.* [online]. 27 October. [Accessed 3 December 2015]. Available at: https://nakedsecurity.sophos.com/2015/10/27/talktalk-breach-ceo-dismisses-encryption-15-year-old-arrested/

9 BIBLIOGRAPHY

Abbott, A. (1988) *The System of Professions: An Essay on the Division of Expert Labor.* Chicago, IL: University of Chicago Press

Accuvant (2014) *Six Forces of Security Strategy* (Clark, J., Christiansen, J., Robinson, J. Guttman, R., Denver). [online]. [Accessed 26 April 2015]. Available at http://www.accuvant.com/resources/accuvants-six-forces-of-security-strategy

ACPO and 7Safe (undated) *Good Practice Guide for Computer-Based Electronic Evidence*. [online]. [Accessed 3 February 2011]. Available at: http://www.7safe.com/electronic_evidence/ACPO_guidelines_computer_evidence.pdf

Adams, D (1996) *Security Survival, A Source Book from The Open Group*, XOpen Company Ltd, New Jersey: Prentice Hall

Adams, J. (1999) *Cars, cholera, and cows: the management of risk and uncertainty*. Cato Policy Analysis No 335. [online]. [Accessed 17 January 2011]. Available at: http://www.cato.org/pubs/pas/pa335.pdf

ALARM (2001) *A key to success – a guide to understanding and managing risk*

Aldridge, M. and Evetts, J. (2003) Rethinking the concept of professionalism: the case of journalism. *British Journal of Sociology* 54(4), pp.547-564

Alemu, G., Stevens, B., Ross, P. and Chandler, J. (2015) The Use of a Constructivist Grounded Theory Method to Explore the Role of Socially-Constructed Metadata (Web 2.0) Approaches, *Qualitative and Quantitative Methods in Libraries (QQML),* 4, pp.517-540

Alred D. (2001) *Awareness, A Never Ending Struggle*, SANS Security Essentials. [online]. [Accessed 1 March 2015]. Available at: http://www.sans.org/reading-room/whitepapers/awareness/awareness-struggle-391

Alter, S. (2002) *IS: Foundation of E-Business.* 4th edition. New Jersey: Pearson Education Inc./Prentice Hall

American Health Information Management Association (2014) *IG Principles for Healthcare (IGPHC).* [online]. [Accessed 3 May 2015]. Available at: http://www.ahima.org/~/media/AHIMA/Files/HIM-Trends/IG_Principles.ashx

Anderson, C. (2010) *The end of theory: Will the Data Deluge Makes the Scientific Method Obsolete?*, WIRED magazine, 23 June 2008

Anderson, P. and James, G. (1999) *Performance Soars, Features Vary.* NetworkWorld. [Accessed 2 February 2011]. Available at: http://www.networkworld.com/reviews/0614rev.html

Anderson, R.J. (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems.* 2nd edition. Indiana: Wiley Publishing Inc.

Andress, M. (2002) *Surviving Security, How to Integrate People, Process and Technology.* Indiana: SAMS Publishing

Anonymous (2001) *Maximum Security, A hacker's Guide to Protecting your internet Site and Network.* 3rd edition. Indiana: SAMS Publishing

Aon Risk Solutions (2014) *Underrated threats? Research into the evolving world of risk.* Aon plc

Archer, H. and Moses, R. (2006) *Delivering and Managing Real World Network Security.* London: BSI

Archives and Records Association UK & Ireland (2010) *Cloud Computing Toolkit: Guidance for outsourcing information storage to the cloud.* [online]. [Accessed 27 March 2011]. Available at: http://www.archives.org.uk/images/documents/Cloud_Computing_Toolkit-2.pdf

Armstrong, L. and Kasinath, G. (2007) *Importance of Verification and Validation of Data Sources in Attaining Information Superiority.* [online]. Originally published in the Proceedings of 5th Australian InfoSec Management Conference. Edith Cowan University. Perth Western Australia. 4 December. [Accessed 2 February 2011]. Available at http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1035&context=ism

Arquilla, J. and Ronfeldt, D. (1997) *In Athena's Camp: Preparing for Conflict in the Information Age.* Washington: RAND

Ashby, S., Palermo, T. and Power, M. (2012) *Risk Culture in Financial Organisations: An interim report.* LSE/Plymouth University

Ashby W.R. (1956) *Introduction to Cybernetics.* Record Number 19571604660. Accessed via CABDirect. [online]. [Accessed 16 August 2015]. Available at: http://www.cabdirect.org/abstracts/19571604660.html;jsessionid=2B1262A529AD5F8C6B08B51080F3A92C

Ashcroft, J. (2001) *Remarks of Attorney General of USA delivered at First Annual Computer Privacy.* Policy & Security Institute. [online]. [Accessed 25 April 2011]. Available at: http://www.justice.gov/criminal/cybercrime/AGCPPSI.htm

Ashford, W. (2014) *European experts divided on success of cybersecurity.* Computer Weekly. [online]. [Accessed 5 October 2015]. Available at: http://www.computerweekly.com/news/2240212945/European-experts-divided-on-success-of-cyber-security

ASIS (2007) *Information Asset Protection Guidelines.* ASIS GDL IAP 05 2007. ASIS International

Aspinall, D. (2004) *An Introduction to IM: The 'Why', 'What' and 'How' of IM, associated legislation and initiatives.* BIP 004. London: British Standards Institution

Atkins, D., Buis P., Hare C., Kelley, R., Nachenberg, C., Nelson, A.B., Phillips, P., Ritchey, T. and Steen, W. (1996) *Internet Security: Professional Reference.* USA: New Riders Publishing

Atos Consulting and National Computing Centre (2007) *Security and Information Risk Survey*

Audit Commission (2009) *Nothing but the truth? A discussion paper.* London: The Audit Commission. [online]. [Accessed 6 February 2011]. Available at: http://www.audit-commission.gov.uk/nationalstudies/localgov/Pages/nothingbutthetruth.aspx

Audit Commission (2010) *The truth is out there, Transparency in an Information Age: A discussion paper.* [online]. [Accessed 7 February 2011]. Available at: http://www.audit-commission.gov.uk/SiteCollectionDocuments/AuditCommissionReports/NationalStudies/20100305thetruthisoutthere.pdf

Australian Public Service Commission (2007) *Tackling wicked problems: A public policy perspective*. Canberra: Australian Government, Commonwealth of Australia

Avižienis, A., Laprie, J. C., Randell, B. and Landwehr, C. (2004) *Basic concepts and taxonomy of dependable and secure computing.* In *IEEE Transactions on Dependable and Secure Computing.* **1**(1), pp.11-33. January-March

Azorin, J.M. and Cameron, R. (2010) *The Application of Mixed Methods in Organisational Research: A Literature Review.* Academic Conferences Ltd

Bach, K. (2004). Pragmatics and the philosophy of language. In L.R. Horn & G. Ward (Eds.), *The handbook of pragmatics.* pp.463-487. Oxford: Blackwell.

Bain, N. and Barker, R. (2010) *the Effective Board: Building individual and board success*. The Institute of Directors. London: Kogan Page

Bamford, J. (2002) *Body of Secrets: How America's NSA and Britain's GCHQ Eavesdrop on the World*. London: Arrow Books

Bankar, P. (2011) Mapping PCI DSS v2.0 With COBIT 4.1. *ISACA Journal.* April. Volume **2**

Banking for International Settlements (2013) *Principles for effective risk data aggregation and risk reporting.* BCBS 239. [online]. [Accessed 2 May 2015]. Available at: http://www.bis.org/publ/bcbs239.pdf

Barlas, C. (2003) Independent consultant - commentary. www.rightscom.com.

Baron, S.M. (2011) Five Questions With..... *ISACA Journal.* Volume **2**

Barrett, D.J. (1996) *Bandits on the information superhighway.* USA: O'Reilly & Associates, Inc

Barrett, N. (2004) *Traces of Guilt*. St Ives: Clays

Bartlett, J. (2015) *The Dark Net*. London: Random House

Baskerville, R.L. and Wood-Harper, A.T. (1996) A critical perspective on action research as a method for IS research. *Journal of IT.* **11**(3), pp.235-246. [online]. [Accessed 17 April 2011]. Available at: http://www.uio.no/studier/emner/matnat/ifi/INF5220/h10/undervisningsmateriale/A_Critical_Perspective_on_Action_Research_as_a.pdf

BBC (2007) *HMRC debacle - UK's families put on fraud alert.* [online]. [Accessed 6 February 2011]. Available at http://tinyurl.com/2mxx94 and http://news.bbc.co.uk/1/hi/uk_politics/7103566.stm

BCS (1999) *E-commerce: A World of Opportunity: A practice guide for professionals & business managers*, Swindon: BCS Publications

BCS (2007) *A Professional Future for IT.* Swindon: BCS Publications

BCS (2008) *Data Guardianship Survey 2008.* Swindon: BCS Publications

BCS (2009) *Plugging the leaks.* Graham Cluley. ITNow. Swindon: BCS Publications. p.12

Bellini, J. (1998) *the information age, Essential business survival strategy for uncertain times.* Berkshire: Business Objects

Benveniste, G. (1987). *Professionalizing the Organization: Reducing Bureaucracy to Enhance Effectiveness*. San Francisco, CA: Jossey-Bass

Bernstein, P.L. (1996) *Against the Gods: The Remarkable Story of Risk.* New York: John Wiley & Sons, Inc.

BERR and PwC (2008) *InfoSec Breaches Survey.* [online]. [Accessed 3 February 2011]. Available at: http://www.pwc.co.uk/eng/publications/berr_information_security_breaches_survey_2008.html

Besse, R.M. (1957) *Company Planning Must be Planned.* In *Dun's Review and Modern Industry.* **74**(4), pp.62-63

Birch, D. (2007) *The Digital Identity Reader, 2007: The best of the Digital Identity Forum Blog.* [online]. London: Mastodon Press. http://www.chyp.com/thought-leaders/blog/

Birch, D. (2008) *The Digital Identity Reader. 2008: A selection of posts from the Digital Identity Forum Blog from 2007 / 2008.* London: Mastodon Press

Bizeul, D. (2007) *Russian Business Network study*

Blair, B.T. (2010) *Making the Case for IG: 10 Reasons Why IG Makes Sense*

Bodley-Scott, S. (2012) *Developing a Thinking Organisation*. Princeton: Kepner-Tregoe, Inc. [online]. [Accessed 31 August 2015]. Available at: http://www.kepner-tregoe.com/pdfs/articles/Thinking_Organisation.pdf

Boddy, D., Boonstra. A. and Kennedy, G. (2005) *Managing IS: An Organisational Perspective.* 2nd edition. (1st edition, 2002). Essex: Pearson Education Ltd. [online]. [Accessed 16 August 2015]. Supporting materials available at: http://www.pearsoned.co.uk/HigherEducation/Booksby/Boddyetal/

Boisot, M. (1987) *Information & Organisations: The Manager as Anthropologist.* London: Fontana Paperbacks

Born, G. (1994) *Process management to Quality Management: The Way to Design, Document and Re-engineer Business Systems.* Chichester: John Wiley & Sons

Borodzicz, E.P. (2005) *Risk, Crisis and Security Management.* Chichester: John Wiley & Sons

Bowen, P., Chew, E. and Hash, J (2007) *InfoSec Guide For Government Executives. CompuSec Division IT Laboratory.* NIST. Gaithersburg. MD20899-8930. [online]. [Accessed 27 February 2011]. Available at: http://csrc.nist.gov/publications/nistir/ir7359/NISTIR-7359.pdf

Bradwell, P. and Gallagher, N. (2007) FYI, *The new politics of personal information: We no longer control what others know about us, but we don't yet understand the consequences.* London: DEMOS

Bradwell, P. (2010) *Private Lives: A People's Inquiry Into Personal Information*. London: DEMOS Report. [online]. [Accessed 3 February 2011]. Available at: http://www.demos.co.uk/publications/privatelives

British-North American Committee (2007) *Cyber Attack: A risk management primer for CEOs and Directors*

Brito, J. and Watkins, T. (2011) *Loving the Cyber Bomb? The Dangers of Threat Inflation in Cybersecurity Policy.* Working Paper No. 11-24. George Mason University: Mercatus Centre

Brotby, W. Krag and Hinson, G. (2013) *Pragmatic Security Metrics: Applying Metametrics to InfoSec.* CRC Press: Bota Raton

Brown, C.V. and Topi, H. (2003) *IS Management Handbook.* 8th edition. Florida: Auerbach Publications

Buchanan, B. (2012) *Plugging the Gaps.* IT Now. Swindon: BCS Publishing

Buckley, R. (2010) *Moving on from the 2007 data loss by HMRC.* [online]. SC Magazine, 25 October. [Accessed 3 February 2011]. Available at: http://www.scmagazineuk.com/moving-on-from-the-2007-data-loss-by-hmrc/article/181676/

Bunker, G. and Fraser-King, G. (2009) *Data Leaks for Dummies.* Indiana: Wiley Publishing, Inc

Burley, D. (2013) *Professionalizing the Nation's Cybersecurity Workforce? Criteria for Decision-Making.* The National Academy of Sciences: National Research Council. [online]. [Accessed 16 August 2015]. Available at: http://www.nap.edu/catalog.php?record_id=18446

Burrell, G. and Morgan, G. (1979) *Sociological Paradigms and Organizational Analysis*. London: Heinemann

Bush, S. F. (2009). *A Brief Letter on Reasoning about IA using the Semantic Web*. In *4th Annual Symposium on IA* (ASIA'09). Volume **2007**, p.36

Business Crime Reduction Centre (BCRC) (2008a) *ICT Security Getting It Right!*

BCRC (2008b) *e-Crime: What your business needs to know.* With Cyber Security Knowledge Transfer Network (KTN)

Business Software Alliance (2003) *InfoSec Governance: Toward a Framework for Action.* Washington: McConnell International, www.mcconnellinternational.com

Butler, C., Rogers, R., Ferratt, M., Miles, G., Fuller, E., Hurley, C., Cameron, R. and Kirouac, B. (2007) *IT Security Interviews Exposed: Secrets to Landing Your Next InfoSec Job.* Wiley Publishing, Inc: Indianapolis

Butler Group (2009) *InfoSec, Protecting the Business.* Butler Group

Calder, A. (2006) *Best Practice: A Management Guide to Implementing InfoSec based on ISO27001/ISO17799.* Zaltbommel: Val Haven Publishing

Cameron, K. (undated) *The Laws of Identity.* [online]. [Accessed 16 August 2015]. Available at: www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

CAMM (2010) *Common Assurance Maturity Model Guiding Principles*, Common Assurance maturity Model Steering Committee

Cappelli, D., Moore, A., Willke, B.J., Shimeall, T.J. and Desai, A.G. (2005) *Management and Education of the Risk of Insider Threat* (MERIT): System Dynamics Modeling of Computer System Sabotage, Carnegie Mellon CyLab, Technical Note: CMU/SEI-2006-TN-041

Cappelli, D.M. and Keeney M. (2004) *Insider Threat: Real Data on a Real Problem.* Presentation. Carnegie Mellon University/United States Secret Service

Capita, CIPFA and Oracle, (2007) *Local Authority Financial Administration Services Emerging Trends in the Context of Shared Services*

Carcary, M. (2009) The Research Audit Trial – Enhancing Trustworthiness in Qualitative Inquiry. *The Electronic Journal of Business Research Methods.* [online]. **7**(1), pp.11-24. [Accessed 17 March 2016]. Available at: www.ejbrm.com

Carnegie, D. (2010) *How to Win Friends and Influence People*, Kindle edition, (originally published 1936)

Carnegie Mellon, (2010) *2010 CERT Research Report,* Software Engineering Institute: Carnegie Mellon. [online]. [Accessed 12 July 2015]. Available at: https://resources.sei.cmu.edu/asset_files/CERTResearchReport/2011_013_001_37704.pdf

Carr, I. (2009) *Computer Crime: The International Library of Criminology, Criminal Justice & Penology.* Second Series. Surrey: Ashgate

Carr, N. (2011) *The Shallows. What the Internet Is Doing to Our Brains*. New York, London: W.W. Norton & Company

Carter, J.A., Clark, A. and Palermos, S.O. (2016) *New Humans? Ethics, Trust and the Extended Mind.* Oxford University Press

Carver, J. and Carver, M. (2001) Carver's Policy Governance® Model in Nonprofit Organizations. Article was originally published as "Le modèle Policy Governance et les organismes sans but lucratif". In the *Canadian Journal Gouvernance - revue international.* [online]. Winter. **2**(1), pp.30-48. [Accessed 31 May 2015]. Available at: http://www.carvergovernance.com/pg-np.htm

Centre for Security Sector Management (2007) *In the Name of National Security Is Britain Well Served?* Cranfield University and CSSM

Chandler, R. (2012) *Corporate Governance and National Prosperity.* New Zealand: Richard Chandler Corporation

Chapman, J. (2008) *'Culture of carelessness': A computer a day goes missing in Whitehall.* Daily Mail. [online]. 29 December. [Accessed 6 February 2011]. Available at: http://tinyurl.com/becxul and http://www.dailymail.co.uk/news/article-1102411/Culture-carelessness-A-day-goes-missing-Whitehall.html

Charmaz, K. (2012) *The power and potential of grounded theory* in *Medical Sociology Online*, **6**(3), pp.2-15. [online]. [Accessed 13 September 2015]. Available at: http://www.medicalsociologyonline.org/resources/Vol6Iss3/MSo-600x_The-Power-and-Potential-Grounded-Theory_Charmaz.pdf

Cheffins, B. (2011) *The History of Corporate Governance,* Legal Studies Research Paper Series: University of Cambridge. Faculty of Law. Paper No. 54/2011. [online]. [Accessed 14 July 2015]. Available at: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1975404

Chen, W. and Hirschheim, R. (2004) A paradigmatic and methodological examination of IS research from 1991 to 2001. *IS Journal.* **14**(3), pp.197-235. doi: 10.1111/j.1365-2575.2004.00173.x

Chickowski, E. (2013) *Using Dependency Modeling for better Risk Decisions*. Dark Reading. [online]. [Accessed 16 August 2015]. Available at: http://www.darkreading.com/risk/using-dependency-modeling-for-better-risk-decisions/d/d-id/1139450?piddl_msgorder=asc

CISCO (2001) *SAFEguarding the E-Business Network: The war against Hackers and Crackers.* Excerpts from the Osborne McGraw-Hill book, Hacking Exposed: Network Security Secrets & Solutions. California: Osborne / McGraw-Hill

CISCO (2015) *Annual Security Report.* [online]. [Accessed 26 April 2015]. Available at: https://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2015_ASR.pdf

CISCO (2001) *SAFEguarding the E-Business Network: The war against Hackers and Crackers.* Excerpts from the Osborne McGraw-Hill book. *Hacking Exposed: Network Security Secrets & Solutions*. California: Osborne / McGraw-Hill

Clarke, R.A. (2005) *The Scorpion's Gate.* New York: G.P. Putnam's Sons

Clarke, R.A. (2007) *Breakpoint.* New York: G.P. Putnam's Sons

Clarke, R.A. (2015) *Pinnacle Event*. New York: St. Martin's Press

Clarke, R.A. and Knake, R.K. (2010) *CyberWar, the next threat to national security and what to do about it.* New York: Ecco/HarperCollins

Clarke-Hill, C.M. and Glaister, K.W. (1995) *Cases in Strategic Management.* 2nd edition. Pitman Publishing

Clegg, S.R. and Palmer, G. (1996) *The Politics of Management Knowledge.* London: SAGE Publications Ltd

Cloud Security Alliance (CSA) (2009) *Security guidance for critical areas of focus in cloud computing. v. 2.1* [online]. [Accessed 16 August 2015]. Available at: http://www.cloudsecurityalliance.org/

ClubCISO (2015) *Information Security Maturity Report 2015: Current information security practice in European organisations*

CSA (2010) *Top Threats to Cloud Computing v.1.0.* [online]. [Accessed 16 August 2015]. Available at: http://www.cloudsecurityalliance.org/

CSA (2010) *Domain 10: Guidance for application security v.2.1*. [online]. [Accessed 16 August 2015]. Available at: http://www.cloudsecurityalliance.org/guidance/csaguide-dom10-v2.10.pdf

CIPFA and PwC (2008) *Shared Services: Where Now? A guide to Public Sector implementation*

Cofta, P. (2013) *Building Trust in InfoSec*, The Alliance of Trustworthy Business Experts / Next Decade Inc. [online]. [Accessed on 24 March 2016]. Available at: http://www.trustacrossamerica.com

Commission of the European Communities (2003) *Establishing the European Network and InfoSec Agency.* C5-0058-03. eEurope 2005

Compliance Consortium (2005) *GRC: An Operational Approach – A Compliance Consortium Whitepaper*. With Bill Zoellick and Ted Frank. Public Draft Version 1.0

Confederation Suisse (2007) *IA Situation in Switzerland and internationally, Semi-annual report 2007/1.* January – June. Feder Office of Police

Conklin, J. (2005) *Chapter 1 of Dialogue Mapping: Building Shared Understanding of Wicked Problems*. In *Wicked Problems and Social Complexity*. CogNexus Institute

Consultative Committee for Space Data Systems (2011) *Audit and Certification of Trustworthy Digital Repositories: Recommended Practice. CCSDS 652.0-M-1.* USA, Washington: Magenta Book

Corder, C. (1985) *Ending the Computer Conspiracy: The Thinking Person's Guide to Successful Systems.* Berkshire: McGraw-Hill Book Company (UK) Ltd

Cornwall, H. and Gold, S. (1989) *New Hackers Handbook.* London: Century

Council of Europe (2008) *Project on Cybercrime*

Cranor, L.R. and Garfinkel, S. (2005) *Security and Usability: Designing Secure Systems That People Can Use.* California: O'Reilly

Creswell, J. W. (2002). *Research design: Qualitative, quantitative, and mixed methods approaches.* 2nd edition. Thousand Oaks, CA: Sage Publications. Chapter 1. [online]. [Accessed 27 November 2011]. Available at: http://www.sagepub.com/upm-data/10981_Chapter_1.pdf

Crosby, Sir J. (2008) *Challenges and opportunities in identity assurance*

Cybersecurity KTN (2008) *Privacy Engineering.* Paper by Marsh, S., Brown, I. and Khaki, M.

Cybersource (2011) *Seventh Annual UK ONLINE FRAUD REPORT.* January edition. Reading: Cybersource

Davis, K. (1977) *Human Behavior at Work, Organisational Behavior*, 5th edition, New York: McGraw-Hill Book Company, pp.384-385

Day, K. (2003) *Inside the Security Mind – Making the tough decisions*, Prentice Hall

Deesing, L. (2015) *What City Officials Need to Know About Cybersecurity.* Techwire. [online]. 24 June. [Accessed 25 June 2015]. Available at: https://www.techwire.net/what-city-officials-need-to-know-about-cybersecurity/

Delamont, S. (2004*) Ethnography and participant observation.* In C. Searle, G. Gobo, J. Gubrium and D. Silverman (eds) *Qualitative Research Practice.* London: Sage. **218**, pp.217-29

Deloitte (2011) *2020: Building the recovery together: What talent expects and how leaders are responding.* Talent Edge

Deloitte (2012) *Risk Intelligence governance in the age of cyber threats: What you don't know could hurt you.* Risk Intelligence Series Issue No. 23

Dennedy, M.F., Fox, J. and Finneran, T.R. (2014) *The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value.* McAfee. Apress Open. [online]. [Accessed 6 September 2015]. Available at: http://link.springer.com/book/10.1007/978-1-4302-6356-2

Detica (2010) *Google, China and cyber security: Practical lessons from the Google hacking incident.* Surrey: Detica Limited

Di Stefano, G., Gino, F., Pisano, G. and Staats, B. (2016) *Making Experience Count: The Role of Reflection in Individual Learning*

Diaz, D.M., Marwick, A.E. and Palfrey, J. (2010) *Youth, Privacy and Reputation.* Literature Review. [online]. [Accessed 16 August 2015]. Available at: http://cyber.law.harvard.edu/publications

DigiTV (2006) *DigiTV The New Citizen Channel for the Digital Age – Delivering Local Government services on Digital Interactive TV.* [online]. [Accessed 24 March 2016]. Available at: www.digitv.org.uk

Digital Policy Alliance (2015) *Post Election Roundtable.* Meeting Minutes. 19 May

Donovan, F. and Bernier, K. (2009) *Cyber Crime Fighters: Tales from the Trenches.* Indiana: Que Publishing

Doswell, B. and Watson, D. (2002) *A Guide to InfoSec Management.* Leicester: Perpetuity Books

Doughty, K. (2001) *Business Continuity Planning, Protecting Your Organization's Life.* Florida: CRC / Auerbach Publications

Duarte, F.J. Fernandes, J. M. and Machado, R. J. (2006) *Business Modeling in Process-Oriented Organizations for RUP-Based Software Development.* In Fettke, P. and Loos, P. (2007) *Reference Modeling for Business Systems Analysis.* Chapter 5. Idea Group Publishing

Dresner, D. (2013) Related blog posts available at: http://www.eradar.eu/author/ddresner/

Drucker, P. (1993) *Management Challenges for the 21st Century.* Harpers Business

Dutton, R. (1995) *Clinical Reasoning in Physical Disabilities*. London: Williams and Wilkins

Eagleton, T. (2033) *After theory*. London: Penguin Books. ISBN: 978-0-14-101507-1

Economic & Social Research Council (2008) *ESRC Seminar Series, Mapping the public policy landscape. The economics of InfoSec.* Cyber Security Knowledge Transfer Network and ESRC. [online]. [Accessed 6 February 2011]. Available at: http://www.abdn.ac.uk/~csc335/ESRC-PPS-EIS.pdf

Edwards, C. (2006) *DEMOS Report, The case for a national security strategy*

Edwards, C. and Fieschi, C. (2008) *UK Confidential – "An open society depends on individuals rediscovering the social value of privacy...".* London: DEMOS

ENISA (2006) *Inventory of risk assessment and risk management methods*. European Network and InfoSec Agency ad hoc working group on risk assessment and risk management

ENISA (2009) *The growing requirement for InfoSec awareness.* Italy: European Communities publishing

ENISA (2009) *Cloud Computing IA Framework*. Available at: http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-information-assurance-framework

ENISA (2010) *Data breach notifications in the EU.* [online]. [Accessed 16 August 2015]. Available at: http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/dbn

Ernst & Young (2003) *Ernst & Young Global InfoSec Survey 2003.* London: Ernst & Young LLP

Ernst & Young (2009) Outpacing *Change Ernst & Young's 12th Annual Global InfoSec Survey.* London: EYGM Limited

EURIM (2002) *E-Crime: A New Opportunity for Partnership, Briefing No 34*

EURIM (2009) *From Toxic Liability to Strategic Asset: Unlocking the Value of Information.* The Information Society Alliance: IG Value of Information Subgroup. [online]. [Accessed 6 February 2011]. Available at: http://www.eurim.org.uk/activities/ig/0911-Value_Summary.pdf

EURIM (2009) *Valuing information as an asset*. London Business School, Chris Higson and Dave Waltho. [online]. [Accessed 17 March 2016]. Available at: http://www.eurim.org.uk/activities/ig/InformationAsset.pdf

EURIM (2010) *Uncovering the Truth: Using information to deliver more for less: A roundtable discussion.* [online]. EURIM/Audit Commission. [Accessed 6 February 2011]. Available at: http://www.eurim.org.uk/activities/ig/100222report.pdf

EURIM (2011) *Report of the Identity Governance* Subgroup. Meeting on 23 February

Evans, M. (2008) *Personal data of 600,000 on lost laptop.* Defence Editor. [online]. 19 January. [Accessed 6 February 2011]. Available at: http://tinyurl.com/b9cto3 and http://www.timesonline.co.uk/tol/news/politics/article3213274.ece

Evans, S. and Pagano, M. (2008) *Exclusive: New batch of terror files left on train - IoS returns confidential documents to Treasury as officials promise to tighten procedures.* [online]. 14 June. [Accessed 6 February 2011]. Available at http://tinyurl.com/5uz98e

Everaert, A. and Mohan, S. (2014*) Decision making in dynamic contexts: A dual perspective approach.* [online]. [Accessed 31 August 2015]. Available at: http://www.adaptivecycle.nl/images/ArjenEveraertEVERAERTMOHANVODCFinalpaper.pdf

Eversheds and Socitm (2000) *E-Government, Best Value and the Law*

Fafinski, S. (2009a) *Garlik UK Cybercrime report.* With 1871 Ltd

Fafinski, S. (2009b) *Computer Misuse: Response, regulation and the law.* Devon: Willan Publishing

Family Health International (2010) *Qualitative Research Methods: A Data Collector's Field Guide, Module 2, Participant Observation*. [online]. [Accessed 13 May 2010]. Available at: *http://www.fhi.org/nr/rdonlyres/ed2ruznpftevg34lxuftzjiho65asz7betpqigbbyorggs6tetjic367v44baysyomnbdjkdtbsium/participantobservation1.pdf*

Farrell, G., Koumpis, C., Maguire, M., Mailley, J., May, A. and Sdralia, V. (2007) *To Err is Human, to Design-Out Divine, Reducing Human Error as a Cause of Cyber Security Breaches.* Cyber Security Knowledge Transfer Network

Fernandez, W.D. (2004) *The Grounded Theory method and case study data in IS research: issues and design.* Australian National University. [online]. [Accessed 3 May 2015]. Available at: http://press.anu.edu.au//info_systems/part-ch05.pdf

Ferrance, E. (2000) *Action Research*, Northeast and Islands Regional Educational Laboratory at Brown University

FFIEC (2016) *Information Technology Examination Handbook, Information Security*, Federal Financial Institutions Examination Council. September 2016

Flechais, I., Mascolo, C. and Sasse, A.M. (2006) Integrating Security and Usability into the Requirements and Design Process. In *International Journal of Electronic Security and Digital Forensics*, *1*(1), pp.12-26. [online]. [Accessed 6 February 2011]. Available at: http://www.cl.cam.ac.uk/~cm542/papers/icges.pdf

Flichy, P. (1993) The Birth of Long Distance Communication. Semaphore Telegraphs in Europe (1790-1840). *Réseaux. The French journal of communication*, **1**(1), p.96

Floridi, L. (2009) The Information Society and Its Philosophy: Introduction to the Special Issue on "The Philosophy of Information, Its Nature, and Future Developments". *The Information Society: An International Journal.* **25**:3, pp.153-158. doi: 10.1080/01972240902848583

Floridi, L. (2014) *Mapping the philosophy of information: A Handbook*

Flynn, N. and Kahn, R. (2003) *E-mail Rules: A Business Guide to Managing Policies, Security and Legal Issues for E-mail and Digital Communication.* New York: American Management Association

Ford, C.L. (2008) New Governance, Compliance, and Principles-Based Securities Regulation. *American Business Law Journal*, **45**(1), pp.1-60. doi: 10.1111/j.1744-1714.2008.00050.x

Forester, T. and Morrison, P. (1994) *Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing.* 2nd edition. London: MIT Press

Foss, R. (2007) Addressing behavioural elements in traffic safety: A recommended approach. *Improving Traffic Safety Culture in the United States; The Journey Forward*. AAA Foundation for Traffic Safety. University of North Carolina at Chapel Hill. [online]. [Accessed 23 March 2016]. Available at: http://trid.trb.org/view.aspx?id=810093

Franscella, J. (2013) *Cybersecurity or Cyber Security?.* infosecisland, blogpost. [online]. [Accessed 29 March 2016]. Available at: http://www.infosecisland.com/blogview/23287-Cybersecurity-vs-Cyber-Security-When-Why-and-How-to-Use-the-Term.html

FRC (2004) *Review of the Turnbull Guidance on Internal Control, Evidence Gathering Phase.* Consultation Paper. Financial Reporting Council

FRC (2010) *The UK Corporate Governance Code.* Financial Reporting Council

FRC (2016) *Corporate Culture and the Role of Boards: Report of Observations*. July 2016

Friedson, E. (1994) *Professionalism reborn: Theory, prophecy and policy*. Oxford: Polity Press.

Friedson, E. (2001) *Professionalism: The Third Logic.* Chicago, IL: University of Chicago Press

FSA (2003) *The firm risk assessment framework*

Funston, F. and Wagner, S. (2010) *Surviving and Thriving in Uncertainty*: *Creating the Risk Intelligent Enterprise.* Indiana: John Wiley & Sons

Furnell, S. (2002) *Cybercrime: Vandalizing the Information Society.* London: Pearson Education/Addison-Wesley

G30 Working Group (2012) *Toward Effective Governance of Financial Institutions.* Washington, DC: The Group of Thirty

Gall, J. (1975) *Systemantics: How Systems Work and Especially How They Fail.* New York: Quadrangle

Gallegos, F., Manson, D.P. and Allen-Senft, S. (1999) *Information Technology Control and Audit.* Florida: CRC Press LLC

Galliers, R.D. and Land, F.F. (1988) *The Importance of Laboratory Experimentation in Information Systems Research - a Response.* Communications of the ACM

Galliers, R. (1992) *Choosing Appropriate IS Research Approaches: A Revised Taxonomy, in* Galliers, R. (ed.) IS Research: Issues, Methods and Practical Guidelines, Blackwell Scientific Publications

Galliers, R.D. (1995) A Manifesto for IM Research. *British Journal of Management.* **6**(s1): S45–S52. doi: 10.1111/j.1467-8551.1995.tb00137.x

Galliers, R.D. (2003*)* Change as crisis or growth? Toward a trans-disciplinary view of IS as a field of study: a response to Benbasat and Zmud's call for returning to the IT artifact. *Journal of the Association for IS.* **4**. pp.337-351

Galliers, R.D. and Leidner, D.E. (2003) *Strategic IM: Challenges and Strategies in Managing IS.* 3rd edition. Oxford: Butterworth Heinemann

Galliers, R., Markus, M.L. and Newell, S. (eds.). (2007) *Exploring IS research approaches: readings and reflections.* Routledge

Galliers, R.D. and Currie, W. (2011) *The Oxford Handbook of Management IS: Critical Perspectives and New Directions* (Oxford Handbooks in Business and Management). OUP: Oxford

Garrett C., (2004) *Developing a Security-Awareness Culture-Improving Security Decision Making.* SANS Institute. [online]. [Accessed 1 March 2015]. Available at: http://www.sans.org/reading-room/whitepapers/awareness/

Garson, G.D. (undated) *Participant Observation and Action Research*, North Carolina State University. [online]. [Accessed 11 May 2010]. Available at: Http://faculty.chass.ncsu.edu/garson/PA765/particip.htm

Gartner (2011) *Embrace Hybrid Thinking to Drive Transformation, Innovation and Strategic Change.* Gartner Inc. G00209217

Gartner (2012) *Survey Analysis: InfoSec Governance.* Tom Scholtz

Gartner (2014) *Survey Analysis: InfoSec Governance*. Tom Scholtz

Gerck, E. (2001) *Trust as Qualified Reliance on Information*. New Jersey: Cook Network Consultants. [online]. [Accessed 6 February 2011]. Available at: http://nma.com/papers/it-trust-part1.pdf

Ghauri P. and Gronhaug, K. (2010) *Research Methods in Business Studies.* 4th edition. (1st edition, 1995). Essex: Pearson Education Ltd

Giddens, Prof. A. (1999) *Reith Lectures.* [Accessed 16 August 2015]. Available at: http://news.bbc.co.uk/hi/english/static/events/reith_99/week2/week2.htm

Girard, K. (2011) *It's Not Nagging: Why Persistent, Redundant Communication Works.* [online]. [Accessed 19 April 2011]. Available at: http://hbswk.hbs.edu/item/6629.html

Goldstein, E. (2000) *The Best of 2600 [A Hacker Odyssey].* Indiana: Wiley Publishing, Inc.

Goodger, A. (2011a) *UK Resilience Blueprint Framework.* Cambridge PhD student

Goodger, A. (2011b) *Why does today's Society need the Information Lodestone.* Cambridge PhD student

Goodger, A. and Atkinson, S. R. (2011a) *Information Lodestone – Understanding, sustaining and nurturing the integrated Information Ecosystem (aka Cyberscape) is the keystone to the UK's existing and future capabilities/abilities),* Cambridge and CESG

Goodger, A. and Atkinson, S. R. (2011b) *Why does today's Society need the Information Lodestone,* Cambridge and CESG

Gorniak-Kocikowska, K. (2008) ICT and the tension between old and new: the human factor. *Journal of Information Communication & Ethics in Society*. **6**(1). Bingley: Emerald Group Publishing Limited, pp.4-27

Gotterbarn, D. and Rogerson, S. (2005). *Responsible Risk Analysis for Software Development: Creating the Software Development Impact Statement*. CAIS.

Gowans Miller, A.D. (2010) *The Maturity of GRC in the Public Sector: Where Are We Today? Where Are We Going?* AGA CPAG Research Series: Report No. 26

Greenberg, E. (2003) *Mission Critical Security Planner: Creating Customized Strategies, When Hackers Won't Take No for an Answer.* Indianapolis: Wiley Publishing Inc.

Greene, R. (2005) *The 48 Laws of Power.* London: Profile Books, The Gap Partnership

Greene, T.C. (2004) *Computer Security for the Home and Small Office.* California: Apress

Guarino, N. (1995) *Formal ontology, conceptual analysis and knowledge representation.* International Journal of Human-Computer Studies. **43**(5), pp.625-640

Hagerty, J. and Kraus, B. (2009) *GRC in 2010: $29.8B in Spending Sparked by Risk, Visibility, and Efficiency.* AMR Research, Inc. [online]. [Accessed 2 May 2015]. Available at: http://www.oversightsystems.com/pdf/whitepapers/AMR-GRC-in-2010.pdf

Hall, P., Heath, C. and Coles-Kemp, L. (2015) Critical visualization: a case for rethinking how we visualize risk and security. *Journal of Cybersecurity*,**1**(1), pp.93-108

Hamadi, R. (2004) *Identity Theft: What it is, How to Prevent it, and What to do if it Happens to You.* London: Vision Paperbacks

Hamill, T.J., Deckro, R.F. and Kloeber, J.M. (2004) *Evaluating IA strategies*. Decision Support Systems. **39** (2005), pp.463-484. Elsevier Ltd

Hansen, L. and Nissenbaum, H. (2009) Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, **53**(4), pp.1155-1175

Hare-Brown, N. (2008) *InfoSec Incident Management – A Methodology.* London: BSI

Harris, S. (2003) *CISSP Certification.* California: McGraw-Hill/Osborne

Hayes, S., Shore, M. and Jakeman, M. (2012) The Changing Face of Cybersecurity. *ISACA Journal.* Volume **6**

Heersmink, R. (2015) *The cognitive integration of scientific instruments: information, situated cognition, and scientific practice*. Phenomenology and the Cognitive Sciences. **1**-21

Herley, C. (2009) *So Long, And No Thanks for the Externalities: The Rational Rejection of Security Advice by Users.* NSPW09. Oxford: Microsoft Research. ACM 978-1-60558-845-2/09/09

Herold, R. (2002) *The Privacy Papers: Managing Technology, Consumer, Employee and Legislative Actions.* Florida: CRC Press LLC

Herrmann, D.S. (2003) *Using the Common Criteria for ITSec Evaluation.* Florida: CRC Press LLC

Hewlett-Packard (2006) *TrustGuide Project: A citizen centric approach to cyber trust: Establishing a dialogue between those that use technology and those that shape technology.* Hazel Lacohee, Stephen Crance and Andy Phippen. Bristol: HP Labs.

Higson, C. and Walthro, D. (2009) *Valuing Information As An Asset.* SAS White Paper. [online]. [Accessed 3 February 2011]. Available at: http://www.eurim.org.uk/activities/ig/InformationAsset.pdf. [Other sources available at: www.eurim.org.uk/activities/ig/voi/voi.php]

Hillson, D. (2014) *The Risk Doctor's Cures for Common Risk Ailments*. Virginia: Management Concepts Press

Hirsch, C. and Ezingeard, J-N (2008) Perceptual and Cultural Aspects of Risk Management Alignment: a case study. *Journal of InfoSec* (JISSec). **4**(1). [online]. [Accessed 16 August 2015]. Available at: http://eprints.kingston.ac.uk/4296/1/Vol4-Is1-1.pdf

Hirschheim, R. (1985) *IS Epistemology: An Historical Perspective*. [online]. London School of Economics. [Accessed 22 September 2015]. Available at: http://ifipwg82.org/sites/ifipwg82.org/files/Hirschheim_0.pdf

Hirschheim, R. and Klein, H.K. (1989) *Four Paradigms of IS Development.* Communications of the ACM. **32**(10), pp.1199–1216

Holt, J. and Newton, J. (2004) *A Manager's Guide to IT Law.* Swindon: BCS Publishing

Holt, J. (2005) *A Pragmatic Guide to Business Process Modelling.* Swindon: BCS Publishing

Hoofnagle, C., King, J., Li, S. and Turow, J. (2010) *How different are young adults from older Adults when it comes to information privacy attitudes & policies?* [online]. [Accessed 16 August 2015]. Available at: http://ssrn.com/abstract=1589864

Hoyle, D. (2009) *Systems and Processes – Is there a Difference?.* [online]. [Accessed 26 April 2015]. Available at: http://www.thecqi.org/Documents/community/South%20Western/Wessex%20Branch/Systems%20and%20Processes%20article%20by%20David%20Hoyle%20Oct09%20%282%29.pdf

HP Security Research (2015) *Cyber Risk Report 2015.* 4AA5-0858ENW. Rev. 2. Art Gilliland

HP (2006) *The HP Security Handbook: Protecting Your Business.* US: Hewlett-Packard Development Company, L.P. 5983-0949ENUS

HP (2008) *The HP Security Handbook: Protecting Your Business.* US: Hewlett-Packard Development Company, L.P. 4AA1-7729EEW

HP (2014) *Protecting Your Business with a More Mature Security Strategy.* In IT Business Edge. [online]. [Accessed 26 April 2015]. Available at: http://www.bitpipe.com/detail/RES/1416257401_440.html

Humphreys, E. (2010) *InfoSec Risk Management – Handbook for ISO/IEC 27001.* BIP 0076. London: BSI

Hurd, Bryan, E. (2001) *The Digital Economy and the Evolution of IS.* Proceedings of the IEEE: 252-257

Hurran, C. (2014) *Cyber Insiders: A Board Issue.* Cyber Security Review. Summer 2014. Institute for Security and Resilience Studies at UCL. 15 May

Huysmans, J. (1998) Revising Copenhagen: Or, On the Creative Development of the Security Studies Agenda in Europe. *European Journal of International Relations*, **12**(3). pp.341-370

I&DeA (2004a) *Answering the call: current HR practice in local authority contact centres research report*

I&DeA (2004b) *Implementing the Freedom of Information Act*. Topic briefing

I&DeA (2004c) *An introduction to Knowledge Management.* Topic briefing

I&DeA (2004d) *Moving forward with Customer Relationship Management*, topic briefing

I&DeA (2004e) *Focusing on improvement – why every project needs a business case,* topic briefing

I&DeA (2004f) *Developing an Access Strategy*, topic briefing

Ibarra, H. (1999) Provisional selves: Experimenting with image and identity in professional adaptation. *Administrative Science Quarterly.* **44**(4). pp.764—791

IBM (2011) *Generally Accepted Recordkeeping Principles (GARP) and how it helps you achieve better IG.* [online]. [Accessed 17 April 2011]. Available at: http://searchcompliance.techtarget.com/feature/FAQ-GARP-and-how-it-helps-you-achieve-better-information-governance

IBM (2014) *Implement a Proactive Strategy for Data Security: Data Security and Privacy are Critical Business Imperatives in the Data Economy.* Forrestor Consulting / IBM

Icove, D., Seger, K. and VonStorch, W. (1995) *Computer Crime: A Crimefighter's Handbook*. O'Reilly & Associates, Inc.

Iivari, J. (1991) A Paradigmatic Analysis of Contemporary Schools of IS Development. *European Journal of IS.* **1**(4), pp.249–272

Iivari, J. (2005) An empirical test of the DeLone-McLean model of IS success. *ACM SIGMIS Database.* **36**(2), pp.8–27

Information Age (2007) *The Effective IT 2007 Report: proven Ways to get the Best from IT.* Information Age

IAAC (2006) *Roadmap for Identity Assurance in the UK*

IAAC (undated) *IA Guidelines for Boards and Senior Managers*

InfoSec and PwC (2010) *InfoSec Breaches Survey.* [online]. [Accessed 3 February 2011]. Available at: http://www.infosec.co.uk/files/isbs_2010_technical_report_single_pages.pdf

Information Security Forum (ISF) (2000a) *Fundamental IRM Implementation Guide.* Reference: 2000/03/01

ISF (2000b) *Fundamental IRM: Supporting Material.* Reference: 2000/03/02

ISF (2002) *Effective Security Awareness Workshop Report.* London: ISF

ISF (2010) *Threat Horizon 2012 - emerging InfoSec threats to business*

InsideCounsel (2014) *The typical data breach lawsuit and how to protect your company.* Sumner and Vervais publish data breach litigation article. [online]. October. [Accessed 14 September 2015]. Available at: http://www.mvalaw.com/news-publications-347.html

Institute of Directors (IoD) (2001) *IA: Protecting your Business in the Information Age.* IoD A Director's Guide. London: Director Publications Ltd

IoD (2005) *InfoSec: Best Practice Measures for Protecting your Business.* IoD A Director's Guide. London: Director Publications Ltd

Institute of Internal Auditors (IIA) (2000) *InfoSec management and Assurance: A Guide for Directors and Executives.* Florida: IIA. Comprising:

1. *InfoSec Management and Assurance: A Call to Action for Corporate Governance*
2. *InfoSec Governance: What Directors Need to Know*
3. *Building, Managing and Auditing InfoSec*

IIA (2008) *International Standards for the Professional Practice of Internal Auditing.* [online]. [Accessed 5 May 2015]. Available at: http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/IOS/temp/IPPF_Standards%20ENG.pdf

IIA Research Foundation (2011) *Improving Organizational Governance Through Implementing Internal Audit Standard 2110.* The Austin Chapter Research Committee

IIA (2012) *Contemporary Practices in Risk Management: Implementation Ideas from Leading Companies.* Audit Executive Center: Special Report, Kathryn Bingham. USA: Florida

Intel (undated) *Moore's Law.* [online]. [Accessed 6 March 2011]. Available at: http://www.intel.com/about/companyinfo/museum/exhibits/moore.htm

Intellect (2005) *i2010 – A European InfoSoc for Growth & Employment*. Intellect's response to the European Commission. Developed as a contribution to the UK Presidency i2010 Conference

International Chamber of Commerce (2003) *InfoSec assurance for executives: An international business companion to the 2002 OECD Guidelines for the security of networks and IS: Towards a culture of security*. France: ICC Publication No. 825. [online]. [Last accessed 24 March 2016]. Available at: http://www.iccwbo.org

Internet Alliance (2000) *An International Policy Framework for Internet Law Enforcement and Security*: An Internet Alliance White Paper

Internet Security Systems (2001) *Simplified Security, SecurePartner Information Guide.* Internet Security Systems, Inc (ISS)

Inthiran, A. and Seddon, A.P. (2007) *Security Models Dissected.* UCTI Working Paper: WP-07-01. [online]. [Accessed 7 October 2010]. Available at http://www.ucti.edu.my/wps/issue2/wp-07-01-paper.pdf

IRM (2011) *Risk Appetite and Risk Tolerance*, *A consultation paper from the Institute of Risk Management.* Richard Anderson

ISACA (2010c) *Monitoring of Internal Controls and IT A Primer for Business Executives, Managers and Auditors on How to Advance Best Practices*. Exposure Draft

(ISC)² (2009) *InfoSecurity Professional*. **3**(7)

(ISC)² (2010a) *InfoSecurity Professional.* **1**(9)

(ISC)² (2010b) *InfoSecurity Professional*. **2**(10)

(ISC)² (2010c) *InfoSecurity Professional*. **3**(11)

(ISC)² (2011a) *InfoSecurity Professional*. **2**(14)

(ISC)² (2011b) *InfoSecurity Professional*. **3**(15)

(ISC)² (2011c) *InfoSecurity Professional*.**4**(16)

(ISC)² (2012a) *InfoSecurity Professional*. **1**(17)

(ISC)² (2012b) *InfoSecurity Professional*. 2(18)

(ISC)² (2012c) *InfoSecurity Professional*. **3**(19)

(ISC)² (2012d) *InfoSecurity Professional*. **4**(20)

(ISC)² (2013b) *InfoSecurity Professional*. **1**(21)

(ISC)² (2013c) *InfoSecurity Professional*. **2**(22)

(ISC)² (2013d) *InfoSecurity Professional*. **4**(24)

(ISC)² (2014a) *InfoSecurity Professional*. **7**(1)

(ISC)² (2014b) *InfoSecurity Professional*. **7**(2)

(ISC)² (2014c) *InfoSecurity Professional*. **7**(3)

(ISC)² (2014d) *InfoSecurity Professional*. **7**(4)

(ISC)² (2014e) *InfoSecurity Professional*. **7**(5)

(ISC)² (2014f) *InfoSecurity Professional*. **7**(6)

(ISC)² (2015a) *InfoSecurity Professional.* **8**(1)

(ISC)² (2015b) *InfoSecurity Professional.* **8**(2)

(ISC)² (2015c) *InfoSecurity Professional*. **8**(3)

(ISC)² (2015d) *InfoSecurity Professional.* **8**(4)

(ISC)² (2015e) *InfoSecurity Professional*. **8**(5)

(ISC)² (2015f) *InfoSecurity Professional*. **8**(6)

(ISC)² (2016a) *InfoSecurity Professional.* **9**(1)

(ISC)² (2016b) *InfoSecurity Professional*. **9**(2)

(ISC)² (2016b) *InfoSecurity Professional*. **9**(3)

(ISC)² (2016b) *InfoSecurity Professional*. **9**(4)

(ISC)² (2016b) *InfoSecurity Professional*. **9**(5)

(ISC)² (2016b) *InfoSecurity Professional*. **9**(6)

(ISC)² (2017a) *InfoSecurity Professional*. **10**(1)

(ISC)² (2017b) *InfoSecurity Professional*. **10**(2)

ISM3 Consortium (2007) *InfoSec Management Maturity Model.* Spain: ISM3 Consortium

ISSA Journal (2016) *The Cyber Profession at Risk: Take Control of Your Cybersecurity Career Life Cycle.* **14**(10), pp.14-15. October 2016

Issacs, L. (2015) *Information governance strategy isn't a project – it's a culture.* [online]. TechTarget blog. [Accessed 3 October 2015]. Available at: http://searchcontentmanagement.techtarget.com/tip/Information-governance-strategy-isnt-a-project-its-a-culture

iStandUK (2017) *Local Public Services Data Handling Guidelines*, Fourth Edition (Revised). February 2017

IT Governance Institute (ITGI) (2001) *Board Briefing on IT Governance.* Illinois: ISACA

ITGI (2002) http://www.itgovernance.org/index2.htm and http://www.itgovernance.org/overview.htm

ITGI (2004) *IT control objectives for Sarbanes-Oxley* and the *IT Assurance Framework.* [online]. [Accessed 3 February 2011]. Available at: http://www.isaca.org/About-ISACA/IT-Governance-Institute/Pages/default.aspx

ITGI (2008) *Val IT Framework 2.0*, ITGI, based on COBIT

Ittner, C.D. and Keusch, T. (2015) *The Influence of Board of Directors' Risk Oversight on Risk Management Maturity and Firm Risk-Taking*.

IWS (2011) *The Information Warfare Site.* National Security Agency, Central Security Service. [online]. [Accessed 7 February 2011]. Available at: http://www.iwar.org.uk/cip/resources/nsa/information-assurance-faq.htm

Jacobson, D. and Rursch, J.A. (2013) *Security Education Climbs the Corporate Ladder.* InfoSec Magazine. TechTarget. **15**(04), p.12

Jaquith, A. (2007) *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* Boston: Addison Wesley

Jellinek, D. (2010) *IM Gaps Highlighted by New Forum.* E-Government Bulletin. 308. [online]. [Accessed 6 February 2011]. Available at: http://www.headstar.com/egblive/?p=428

Jenkins, G.H. (1997) *IS: Policies and Procedures Manual.* New Jersey: Prentice-Hall Inc.

Jericho Forum (2007) *Jericho Forum Commandments.* Version 1.2. [online]. [Accessed 26 April 2015]. Available at: https://collaboration.opengroup.org/jericho/commandments_v1.2.pdf

Johnson, R.A. (2008) *Management, systems, and society: an introduction. Picture.* [online]. [Accessed 6 June 2011]. Available at: http://upload.wikimedia.org/wikipedia/commons/c/c5/Systems_Model_of_Action-Research_Process.jpg

Joint Economic Committee (2002) *Security in the Information Age: New Challenges. New Strategies.* United States Congress

Jones, A. and Ashenden, D. (2005) *Risk Management for Computer Security*, *Protecting Your Network and information Assets,* Oxford: Elsevier Butterworth Heinemann

Jones, A., Kovacich, G.L. and Luzwick, P.G. (2002) *Global Information Warfare: How Businesses, Governments, and Others Achieve Objectives and Attain Competitive Advantages.* Florida: CRC Press Plc

Jones, V. (2010) *Risk Decisions.* [online]. 12 May. [Accessed 23 March 2016]. Available at: http://www.enterpriseriskmag.com/

Jurgens, M. (2007) *The 4 Pillars of Innovation in IT.* 2nd edition. Epe: Drukkerij Hooijberg

Kalfoglou, Y. and Schorlemmer, M. (2003) *Ontology mapping: the state of the art*. In *The knowledge engineering review*. **18**(01), pp.1-31

Kaplan, S.J. (1968) *The advancing communication technology and computer communication systems.* Western Union, Mahwah, New Jersey

Kapoor, G. and Brozzetti, M. (2010) The Transformation of Internal Auditing: Challenges, Responsibilities and Implementation. *The CPA Journal*

Keep IT Secure (2007) *cyber-crime The Risks Explained, A Rough Guide in Plain English for Non-Technical Readers.* Edition 1

Killmeyer, J. (2006) *InfoSec Architecture: An Integrated Approach to Security in the Organization.* 2nd edition. Florida: Auerbach Publications

Kirschenbam, A., Mariani, M., Van Gulijk, C., Lubasz, S., Rapaport, C. and Andriessen, H. (2012) Airport Security: An ethnographic study. *Journal of Air Transport Management.* **18**(1). pp.68-73. Elsevier Ltd

Knight, F. H. (2012) *Risk, uncertainty and profit.* Courier Corporation

Kobus, W.S. (2002) *Security Solutions: Thinking Outside the Box – Building a Leading-Edge Security Management Program.* Total Enterprise Security Solutions, LLC

Koontz, H., O'Donnell, C. and Weihrich, H. (1980) *Management.* 7th edition. New York: McGraw-Hill

Kotter, J. (2013) *Management is (still) not Leadership*. [online]. [Accessed 14 July 2015]. Available at: http://blogs.hbr.org/kotter/2013/01/management-is-still-not-leadership.html?cm_mmc=email-_-newsletter-_-leadership-_-leadership020513&referral=00206&utm_source=newsletter_leadership&utm_medium=email&utm_campaign=leadership020513

KPMG (2012) *A nuanced perspective on Cybercrime: Shifting viewpoints, call for action,* KPMG Advisory N.V. [online]. [Accessed, 26 April 2015]. Available at: https://www.kpmg.com/TT/en/IssuesAndInsights/ArticlesPublications/Documents/Nuanced-Perspective-on-Cybercrime-Art.pdf

KPMG (2013) *Five move common cyber security mistakes: Management's perspective on cyber security.* KPMG Advisory N.V. [online]. [Accessed, 26 April 2015]. Available at: https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/five-most-common-cyber-security-mistakes.PDF

KPMG (2015) *FTSE 350 Cyber Governance Health Check: An insight into the issues of today and tomorrow.* Oliver for KPMG. OMO25060A

Kral, R. (2011) *Decision Rights and Information Flows.* Candela Solutions LLC. [online]. 27 July. Article reprint from the Governance Issues Newsletter. **2011**(3). [Accessed 26 April 2015]. Available at: http://www.candelasolutions.com/ace-files/Decision_Rights_and_Information_Flows.pdf

Kreiner, G.E., Ashforth, B.E. and Sluss, D.M. (2006a) Identity dynamics in occupational dirty work: Integrating social identity and system justification perspectives. *Organization Science.* **17**(5), pp.619-636

Kreiner, G.E., Hollensbe, E.C. and Sheep, M.L. (2006b) Where is the 'Me' among the 'We'? Identity work and the search for optimal balance. *Academy of Management Journal.* **49**(5), pp.1031-1057

Kroes, R. and Meijers, A. (2000a) Guest editor's preface. In R Kroes & A. Meijers (Eds.), *The empirical turn in the philosophy of technology* (p. xv). Amsterdam: JAI/Elsevier

Krutz, R.L. and Vines, R.D. (2003) *The CISM Prep Book.* Indiana: Wiley Publishing, Inc.

Kushner, L. and Murray, M. (2010) *Do you have the intangibles?* InfoSec Magazine. pp.36-44

Lacey, D. (2008) *Talking about a revolution.* Infosecurity. Elsevier

Lacey, D. (2010) *Responding to the New Information Risk Landscape: New priorities, New skills and New solutions.* Qualys. [Accessed 3 February 2011]. Available at: http://whitepapers.theregister.co.uk/paper/view/1625/qualys-responding-to-the-new-info-risk-landscape.pdf

Lacey, D. (2011) *Nine Steps to Smart Security for Small Businesses.* Qualys

Lacey, D. and James, B.E. (2010) *Review of Availability of Advice on Security for Small/Medium Sized Organisations.* ICO

Lafley, A.G. and Martin R.L. (2013) *Playing Win: How Strategy Really Works*. Harvard Business Review Press: Massachusetts

Lan, M., Gang, L. and Wei, G. (2010) *State observer based adaptive IA evaluation model*, in *Wireless Communications, Networking and InfoSec (WCNIS).* [online]. 2010 IEEE International Conference. pp.173,178. doi: 10.1109/WCINS.2010.5541914. [Accessed 31 May 2015]. Available at: http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5541914&isnumber=5541718

Larstan (2005) *Larstan's The Black Book on Corporate Security*. Potomac MD: Larstan Publishing

Lawson, S. (2012) Putting the "war" in cyberwar: Metaphor, analogy, and cybersecurity discourse in the United States. *First Monday*, **17**(7)

Leech, T.J. (1998) *Control & Risk Self-Assessment: The Dawn of a New Era In Corporate Governance* (Originally published 1990)

Leech, T.J. (2012) *The High Cost of "ERM Herd Mentality".* White Paper. Canada: Risk Oversight

Lehrer, J. (2010) *The Truth Wears Off – Is there something wrong with the scientific method?* [online]. [Accessed 19 April 2011]. Available at: http://www.newyorker.com/reporting/2010/12/13/101213fa_fact_lehrer

Lepisto, D.A., Crosina, E. and Pratt, M.G. (2015) Identity work within and beyond the professions: Toward a theoretical integration and extension. *International Handbook about Professional Identities.* pp.203-222

Lewin, K. (1943) Defining the Field at a Given Time. In *Psychological Review.* **50**(3), pp.292-310, Republished in *Resolving Social Conflicts & Field Theory in Social Science.* Washington, D.C.: American Psychological Association. 1997

Lewin, K. (1946) Action Research and Minority Problems. *Journal of Social Issues.* **2**, pp34-46

Levy, I. (2011) *Government systems: how much security is enough?* Government Computing. Guardian article. [online]. 25 October. [Accessed 24 March 2016]. Available at: http://www.guardian.co.uk/government-computing-network/2011/oct/25/cesg-information-assurance-government/print

Litchko, J.P (2004) *Know IT Security: Secure IT Systems Casino Style.* Kensington: Know Book Publishing

Litchko, J.P. and Payne, A. (2004) *Know Cyber Risk by Managing Your IT Security!* Kensington: Know Book Publishing

Liu, P., Meng, Y. and Jiwu, J. (2014) *IA.* Penn State. [Accessed 21 June 2015]. Available at: s2.ist.psu.edu/paper/82-info-assurance-v6.pdf

Livingston, G. (2011) *The Definitive Guide to Business Continuity Planning.* MIR3. [online]. [Accessed on 12 May 2011]. Available at: www.mir3.com

Loeb, L. (2001) *IA Powwow*: Conference at West Point focuses on the challenges of IA. Secure Electronic Transactions

London, K.R. (1976) *The People Side of Systems – the human aspects of computer systems*. Maidenhead, Berkshire: McGraw-Hill

London School of Economics and Political Science (2009) *Briefing on the Interception Modernisation Programme.* [online]. [Accessed 1 March 2015]. Available at: http://www.lse.ac.uk/management/documents/IMP-briefing.pdf

Lowenthal, P. R. and Leech, N. (undated) Mixed research and online learning: Strategies for improvement. *Press*

Lumension (2012) *What every CEO should know about IT Security.* Scottsdale. [online]. [Accessed 26 April 2015]. Available at: https://www.lumension.com/Resources/eBooks/what-every-ceo-should-know-about-it-security.aspx

Lyon, D. (2001) *Surveillance Society: Monitoring everyday life.* Buckingham: Open University Press

Madse, P. and Shafritz, J. (eds) (1991) *Essentials of Business Ethics.* New York: Meridian

Magnin, C.J. (2001) *The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?*

Mahboobi, J.R. (2001) *Cyber Governance: Who will Tame the Shrew!* [online]. NETMAG. July-August. [Accessed on 20 April 2011]. Available at: http://www.marvelsystem.com/downloads/cybergovernance.pdf

Maiwald, E. and Sieglein, W. (2002) *Security Planning & Disaster Recovery.* California: McGraw-Hill/Osborne

Marakas, G.M. and O'Brien, J.A. (2008) *Introduction to IS,* 14th edition. New York: McGraw-Hill Irwin

March, S., Brown, I. and Khaki, M. (2008) *Privacy Engineering.* Cybersecurity KTN

Marks, N. (2015) *How much cyber risk should you take?* Norman Marks on Governance, Risk Management and Audit blog. [online]. [Accessed 14 September 2015]. Available at: https://normanmarks.wordpress.com/2015/05/24/how-much-cyber-risk-should-you-take/

Marks, N. (2015) *World-Class Risk Management.* Marston Gate: Amazon

Marsh (2011) *Preparing the local public sector for risk governance: First steps towards an ISO31000 framework – Framework for public risk governance and lessons learnt*

Mason, R. O., McKenney, J.L. and D.G. Copeland (1997b) *An Historical Method for MIS Research: Steps and Assumptions.* MIS Quarterly. September

Matthews, J. (2003) 'A framework for the creation of practitioner-based evidence', *Education and child Psychology,* **20**(4): 60-7

Mattord, H.J. and Whitman, M.E. (2005) *Principles of InfoSec.* 2nd edition

Mayo, E. and Steinberg, T. (2007) *Power of Information Review.* [online]. [Accessed 17 March 2016]. Available at: http://www.opsi.gov.uk/advice/poi/power-of-information-review.pdf

McAfee (2005) *Virtual Criminology Report: The first pan-European study into organised crime and the internet*

McCarthy, L. (2003) *IT Security: Risking the Corporation.* New Jersey: Prentice Hall

McConnell, C. (2002) *Change Activist: Make Big Things Happen Fast.* London: Pearson Education Ltd with Momentum

McConnell, M. (2002) *IA in the Twenty-First Century.* (Supplement to Computer Magazine), Computer. (4). pp.16-19

McCumber, J. (2004) *Assessing and Managing Security Risk in IT Systems: A Structured Methodology.* Florida: Auerbach Publications

McKee, A. (2003) *Textual analysis: A beginner's guide*. Sage

McKilligan, N.F.J. and Powell, N.H.E. (2009) *Data Protection Pocket Guide: Essential Facts at Your Fingertips.* 2nd edition. BIP 0050. London: BSI

McMullan, T. (2015) *What does the panopticon mean in the age of digital surveillance?* [online]. 23rd July 2015. [Accessed 28 January 2017]. Available at: https://www.theguardian.com/technology/2015/jul/23/panopticon-digital-surveillance-jeremy-bentham

McNiff, J. (2002) *Action research for professional development: Concise advice for new action researchers.* 3rd edition

Miller, D. and Woodman, M. (2015) Reconceptualizing the IT Delivery Model and the Role of Enterprise Architect. *The Journal of IT Management.* Cutter IT Journal. **28**(2)

Mingers, J. (2003) The paucity of multimethod research: a review of the IS literature. *IS Journal.* **13**(233–249). doi: 10.1046/j.1365-2575.2003.00143.x

Mitchell, J. (2013) Take Control. *ITNow*. Swindon: BCS Publishing

Mitnick, K.D. and Simon, W.L. (2002) *The Art of Deception: Controlling the Human Element of Security.* Indiana: Wiley Publishing, Inc.

Mitrakas, A. (2011) Assessing liability arising from InfoSec breaches in data privacy. *International Data Privacy Law.* **1**(2), p.129

Monroe, R. (2015) *Compliance is Like Asking Your Kids to Clean Their Room.* Blog Post. [online]. [Accessed 14 September 2015]. Available at: http://darkmatters.norsecorp.com/2015/05/25/compliance-is-like-asking-your-kids-to-clean-their-room/

MORI Social Research Institute (2005) *e-Democracy Survey 2005. Local authorities experiences of democracy on and off line*

MORI market dynamics (2005) *What works – Key lessons from recent e-Democracy literature.* January

Morris, J. (2006) *Practical Data Migration.* Swindon: BCS Publishing

Munley M. (2004) *Moving from Consciousness to Culture: Creating an Environment of Security Awareness.* [online]. SANS Institute. [Accessed 1 March 2015]. Available at http://www.sans.org/reading-room/whitepapers/awareness/

Murphy, B. (2006) *IM 101: How to Tackle An Enterprise IM Strategy,* Forrester Best Practices series. Forrester Research Inc.

National Computing Centre (NCC) (2000) *Business InfoSec Survey* (BISS). Conducted in 1999. Manchester: The NCC

NCC (2002) *Managing Risk: A Practical Guide.* Guidelines for IT Management 265. W. Morton. Manchester: The NCC

NCC (2003) *Survey: Risk Management in IT.* Manchester: The NCC

NCC (2004b) *Biometrics.* Manchester: The NCC

NCC (2004c) *InfoSec Policy and Practice.* Manchester: The NCC

NCC (2005) *An analysis of surveys for the Small Business Service of the DTI.* Manchester: The NCC

NCC (2006) *User Authentication.* Manchester: The NCC

NCC (2007) *Information Availability.* Manchester: The NCC

National Hi-tech Crime Unit (2004) *Hi-Tech Crime: The Impact on UK Business*.

National Performance Management Advisory Commission (2010) *A Performance Management Framework for State and Local Government: From Measurement and Reporting to Management and Improving.* USA: Chicago

Newsted, P.R., Chin, W., Ngwenyama, O. and Lee, A. (1996) *Resolved: Surveys have Outlived their Usefulness in IS Research.* In Proceedings of the 1996 International Conference on Information Systems. Cleveland, Ohio

Newsted, P.R., Huff, S. and Munro, M. (1998*) Survey Research in IS.* MISQ Discovery

Nichols, R.K., Ryan, D.J. and Ryan, J.J.C.H. (2000) *Defending your digital assets against hackers, crackers, spies & thieves.* New York: McGraw-Hill, Inc.

NoticeBored (2008) *InfoSec Awareness Briefing Pack for Software Developers* from NoticeBored. Available at www.noticebored.com

OECD (2004) *OECD Principles of Corporate Governance.* Organisation for Economic Co-Operation and Development. Paris

OECD (2005) *Task Force on Spam: Anti-Spam Law Enforcement Report.* J00184175 DSTI/CP/ICCP/SPAM(2004)3/FINAL

OCEG (2007) *Internal Audit Guide: Assessing Governance, Risk, Compliance and Ethics Capabilities (OIAG).* Version 1.0. Arizona: Open Compliance & Ethics Group

OCEG (2009b) *GRC Reference Architecture: Enterprise Data Architecture & Framework.* Open Compliance and Ethics Group. [Accessed 26 April 2015]. Available at: http://grc2020.com/2009/11/05/76grc-reference-architecture-enterprise-data-architecture-framework/

OCEG (2011) *GRC* Open Compliance and Ethics Group. [online]. [Accessed 27 February 2011]. Available at: www.oceg.org

OCEG (2015) *OCEG Red Book GRC Capability Model: Achieving Principled Performance by integrating the governance, assurance and management of performance, risk and compliance.* Version 3.0. Scott Mitchell, Carole Switzer and Jason Mefford. [online]. [Accessed 17 March 2016]. Available at: http://www.oceg.org/resources/red-book-3/

Ogren, J.G. and Langevin, J.R. (1999) *Responding to the threat of cyberterrorism through IA*. Naval Postgraduate School Monterey CA

O'Hara, K. and Shadbolt, N. (2008) *The Spy in the Coffee Machine*. Oxford: Oneworld

Omand, D. (2010) *Securing the State.* London: C. Hurst & Co (Publishers) Ltd

Onwuegbuzie, A.J. and Burke Johnson, A. (2004) *Mixed Methods Research: A Research Paradigm Whose Time Has Come.* Educational Researcher

Onwuegbuzie, A.J. and Leech, N.L. (2006) *Linking research questions to mixed methods data analysis procedures.* The Qualitative Report. **11**(3), pp.474-498. [online]. [Accessed 27 November 2011]. Available at http://www.nova.edu/ssss/QR/QR11-3/onwuegbuzie.pdf

OpenText (2009) *FTP: The enemy within*, in association with Connectivity Solutions Group. [online]. [Accessed 16 August 2015]. Available at: http://connectivity.opentext.com/resource-centre/whitepapers/ftp-the-enemy-within-1.aspx

Oppliger, R. (1998) *Internet and Intranet Security.* Boston: Artech House

Oqvist, K.L. (2009) *Your Privacy in the InfoSoc.* Swindon: BCS Publishing

Osterman Research White Paper (2011) *The Global Malware Problem: Complacency can be Costly.* [online]. [Accessed 17 March 2016]. Available at: http://www.ostermanresearch.com/downloads.htm#Security

OWASP (2010) *Open Web Application Security Project: Top Ten Project*. [online]. [Accessed 4 February 2011]. Available at: http://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

PA Consulting (2011) *Tackling the Challenges of Cyber Security: Taking an Integrated Approach to Protecting your Business.* Security Integration and Protective Monitoring (SIPM). [online]. [Accessed 3 October 2015]. Available at: http://www.paconsulting.com/business-challenges/cyber-security/

Pariser, E. (2011) *The Filter Bubble, What the Internet is Hiding from You.* London: Penguin Books

Park, S. and Ruighaver, T. (2008) *Strategic Approach to InfoSec in Organizations.* ICISS, pp.26-31. International Conference on Information Science and Security (ICISS 2008). [online]. [Accessed 3 February 2011]. Available at: http://www.computer.org/plugins/dl/pdf/proceedings/iciss/2008/3080/00/30800026.pdf?template=1&loginState=2&userData=AMA%2BInternational%2BUniversity%253AAMA%2BInternational%2BUniversity%253AAddress%253A%2B80.42.155.243%252C%2B%255B172.16.161.5%252C%2B80.42.155.243%255D

Parker, D.B. (2002) *Motivating the Workforce to Support Security Objectives: A Long-Term View.* [Based on Chapter 16, "Fighting Computer Crime, A New Framework for Protecting Information". By Donn Parker and published by John Wiley & Sons, 1998]

Paul, R. (2005) *The state of critical thinking today,* New directions for community colleges. **2005**(130), pp.27-38

Pedley, P. (2003) *essential LAW for information professionals.* London: Facet Publishing

Peters, T. (2003) *Re-imagine! Business Excellence in a Disruptive Age.* London: Dorling Kindersley

Pipkin, D.L. (1997) *Halting the Hacker: A Practical Guide to Computer Security.* New Jersey: Prentice Hall

Pitt-Payne, J. (2010) *Information Law in the New Parliament.* 11kbw

POA Publishing LLC (2003) Asset Protection and Security Management Handbook. USA: Auerbach Publishing

Powell, R., Holmes, T.K. and Pie, C.E. (2010) *The information assurance range*. Defense Information Systems Agency, Falls Church VA

Power, M., Ashby, S. and Palermo, T. (2013) Risk Culture in Financial Organisations. *London School of Economics,* London. [online]. [Accessed 12 July 2015]. Available at: http://sydney.edu.au/business/__data/assets/pdf_file/0017/212624/2014_Power_Abstract.pdf

Pratt, M.G., Rockmann, K.W. and Kaufmann, J.B. (2006) Constructing professional identity: The role of work and identity learning cycles in the customization of identity among medical residents. *Academy of Management Journal,* **49**(2), pp.235-262

PriceWaterhouseCoopers (2006) *8th Annual Global CEO Survey: Bold Ambitions, Careful Choices.* [online]. [Accessed 3 May 2015]. Available at: https://www.pwc.ch/user_content/editor/files/publ_corp/pwc_08th_annual_global_ceo_survey_e.pdf

PriceWaterhouseCoopers (2010) *Revolution or evolution? InfoSec 2020.* Technology Strategy Board [T10/037]

PriceWaterhouseCoopers (2010) *Preparation Perseverance Payoff - Implementing a combined assurance approach in the era of King III.* Business School, Risk Assurance. www.pwc.com/za

Privacy Laws & Business (2010) *Newsletter*, Issue 50

Privacy Rights Clearinghouse (2008) *A chronology of data breaches reported since the choicepoint incident (list)*. Available at: http://www.privacyrights.org/ar/ChronDataBreaches.htm

Provencher, C. (2009) *InfoSec Governance Architecture*, in ISO/IEC Information & ICT Security and Governance Standards in practice, Ottawa Panel Session Standards presentation

Protiviti (2010) *The Global Privacy and InfoSec Landscape, Frequently Asked Questions*, Protiviti Inc, PRO-0310-101027, www.protiviti.com

Quick, C. (2012) *Redefining Information Assurance Compliance*. Army Signal Centre of Excellence, Fort Gordon GA

Ranum, M. and Schneier, B. (2010) *Should enterprises give in to consumerization at the expense of security?* Face-Off. InfoSec Magazine

Raval, V. (2012) Changing Times and Eternality of Ethics. *ISACA Journal*. Volume **2**, p.9

Raval, V. and Dyche, G. (2012) Seven Myths of Information Governance. *ISACA Journal.* Volume **4**, p.26

Rapoport, R. (1970) Three dilemmas in action research. *Human Relations.* **23**(6), pp.499-513

Rasmussen, M. (2006) *Taking Control of IT Risk: Defining a comprehensive IT Risk Management Strategy.* Forrester Best Practices series. Forrester Research Inc.

Remenyi, D. Williams, B., Money, A. and Swartz, E (1998) *Doing Research in Business Management: An Introduction to Process and Method.* London: Sage Publications

Rice, D. (2008) *Geekonomics: The Real Cost of Insecure Software.* Boston: Addison Wesley

Richardson, G. (undated) *IDeA: marketplace, A Lever Long Enough: Using the internet to enhance local government procurement*

Rid, T. (2013) *Cyber War Will Not Take Place.* London: C. Hurst & Co. (Publishers) Ltd

Robson, W. (1997) *Strategic Management and Information Systems.* 2nd edition. Essex: Pearson Education Ltd – Prentice Hall/Financial Times

Room, S. (2007) *Data Protection and Compliance in Context.* Swindon: BCS Publishing

Rosenoer, J. (1997) *Cyber Law, The Law of the Internet.* New York: Springer-Verlag

Ross, S.J. (2011) What is the Value of Security? *ISACA Journal.* Volume **2**

Rothke, B. (2004) *Computer Security: 20 Things Every Employee Should Know.* New York: McGraw-Hill Professional Education

Rousmaniere, K. (2004) *Historical research*. [online]. In K. deMarrais & S. D. Lapan (eds.) *Foundations for research.* pp.31-50. Mahwah, NJ: Lawrence Erlbaum Associates. [Accessed 27 November 2011]. Available at: http://www4.nau.edu/cee/ci_doc/current/resources/2_Rousmaniere.pdf

Royal Academy of Engineering (2006) *Report and proceedings of a seminar on: The Economics and Morality of Safety.* 16 February. London: The Royal Academy of Engineering

Royal Academy of Engineering (2007a) *Dilemmas of Privacy and Surveillance: Challenges of Technological Change*. March. London: The Royal Academy of Engineering

Royal Academy of Engineering (2007b) *Engineering Ethics in Practice* seminar and papers. 13 June

Royal and Sun Alliance (2001) *Risk Control Note No. 11 Protecting Computers and Other Electronic Office Equipment Against Theft*. RCH11. Issue 3

RSD (2014) *The Authoritative Guide to Information Governance,* RSD Glass

Sabett, R.V. (2015) Look, Up in the Sky, It's... Pigs???, In *ISSA Journal.* **13**(1), p.5

Samson, S.A. (1994) *Models of Historical Interpretation*, Contra Mundum, No. 11, Spring

Sandis, C. (2016) *Philosophy's influence on technology design—and why it needs to change*, February 12, University Of Hertfordshire, The Conversation

SANS (2001) *Awareness, A Never Ending Struggle*, SANS Institute InfoSec Reading Room

SANS (2004) *Moving from Consciousness to Culture: Creating an Environment of Security Awareness.* SANS Institute InfoSec Reading Room. Mary Munley. Version 1.4b

SANS (2004) *Developing a Security-Awareness Culture – Improving Security Decision Making.* SANS Institute InfoSec Reading Room

Scambray, J., McClure, S. and Kurtz, G. (2001) *Hacking Exposed: Network Security Secrets and Solutions.* 2nd edition. New York: McGraw-Hill

Schifreen, R. (2006) *Defeating the Hacker: A Non-Technical Guide to IT Security.* Chichester: John Wiley & Sons Ltd

Schneier, B. (2000) *Secrets and Lies: Digital Security in a Networked World*. New York: John Wiley & Sons

Schneier, B. (2012) *Liars and Outliars: Enabling the Trust that Society Needs to Thrive.* New Jersey: Wiley

Schneier, B. (2013a) *Power and the Internet.* Cryptogram. [online]. [Accessed 17 March 2016]. Available at: https://www.schneier.com/crypto-gram/archives/2013/0215.html#1

Schneier, B. (2013b) *People, Process, and Technology.* [online]. [Accessed 2 October 2015]. Available at: https://www.schneier.com/blog/archives/2013/01/people_process.html

Schwartau, W. (1994) *Information Warfare: Cyberterrorism - Protecting your personal security in the electronic age.* New York: Thunder's Mouth Press

SEC (2007) *SEC 2007 Commission Guidance Regarding Management's Report on Internal Control Over Financial Reporting.* [online]. [Accessed 16 August 2015]. Available at: http://www.sec.gov/rules/interp/2007/33-8810.pdf

Seger, K.A. (2003) *Utility Security: The New Paradigm.* Oklahoma: PennWell Corporation

SFIA Foundation (2008) *Skills Framework for the Information Age v4*. UK

Shah, S. (2015) *The 10 worst-ever government IT projects.* [online]. [Accessed 23 September 2015]. Available at: http://www.computing.co.uk/ctg/feature/2422715/the-10-worst-ever-government-it-projects

Shannon, C. E. and Weaver, W. (1949) *The mathematical theory of information*

Sheldrake, J. (1996) *Management Theory from Taylorism to Japanization.* Thomson Learning

Shirky, C. (2010) *Cognitive Surplus: Creativity and Generosity in a Connected Age.* London: Penguin

Simon, H.A. (1991) *Bounded rationality and organizational learning*, Organization Science. **2**(1), pp.125-134

Singh, P.K. (2017) *Kill that CISO – A CEO's guide*. [online] February 8. LinkedIn

Slade, R. (2006) *Dictionary of Security.* Canada: Syngress

Slay, H. and Smith, D.A. (2011) Professional identity construction: Using narrative to understand the negotiation of professional and stigmatized cultural identities. *Human Relations,* **64**(1), pp.85-107

Smith, M. (2012) IA. *Database and Network Journal.* **13**+. *Expanded Academic ASAP*. GALE|A229835813

Socitm Insight (2001) *Local e-government: learning from the best*

Socitm Insight (2003a) *Rediscovering knowledge: An overview of knowledge sharing in the public sector*

Socitm Insight (2003b) *Big successes by small councils – some shining examples of e-government achievement in shire districts*

Socitm Insight (2003c) *Charting Information: An overview of IM in the public sector.* November

Socitm Insight (2004a) *Steering a safe passage, An update on the legal implications of managing information*

Socitm Insight (2005a) *Efficiency, transformation and the council website, A briefing for elected members, chief executives and senior managers*

Socitm Insight (2005b) *E is for efficiency, Reaping the benefits of technology*

Socitm Insight and CIPFA (2005) *A marriage of convenience? A review of experiences from partnerships and outsourcing contracts*

Souag, A, Salinesi, C. and Wattiau, I. (2012) *Ontologies for Security Requirements: A Literature Survey and Classification* (long version). [online]. <hal-00709970>. [Accessed 24 June 2015]. Available at: https://hal.archives-ouvertes.fr/hal-00709970/document

Spinello, R.A. (2003) *Cyber Ethics: Morality and Law in Cyberspace.* 2nd edition. London: Jones and Bartlett Publishers

Stahl, B.C., Shaw, M. and Doherty, N. (2008) *IS Security Management: A Critical Research Agenda.* Association of IS, ISGSEC Workshop on InfoSec & Privacy (WISP 2008). Paris

Stair, R.M. and Reynolds, G.W. (2006) *Principles of IS.* Massachusetts: Thomson Course Technology

Stamp, M. (2006) *InfoSec: Principles and practice.* New Jersey: John Wiley & Sons Inc.

Statman, M. (2010) *The culture of risk tolerance* [online]. [Accessed 13 September 2015]. Available at: http://ssrn.com/abstract=1647086 (SSRN-id1647086)

Stephenson, P. and Prueitt, P.S. (2005) *Applied Different Ontology Framework: Bringing the knowledge of concepts to IA and Cybersecurity Using FARES.* Draft Version 1.0. Ontology Tutorial 7

Stevens, J.A. (2005) *Information Asset Profiling.* Carnegie Mellon University. CMU/SEI-2005-TN-021

Stevens, T. (2011) *The Department of 'No'*, The Privacy, Identity & Consent Blog. [online]. Computer Weekly. [Accessed 26 February 2011]. Available at: http://www.computerweekly.com/blogs/the-data-trust-blog/2011/02/the-department-of-no.html

Stigler, G.J. (1961) *The Economics of Information.* [online]. In *The Journal of Political Economy.* pp.213-225 [Accessed 13 September 2015]. Available at: http://home.uchicago.edu/~vlima/courses/econ200/spring01/stigler.pdf

Stoll, C. (1989) *The Cuckoo's Egg.* Doubleday

Straub, D.W. (1989) *Validating Instruments in MIS Research.* MIS Quarterly. **13**(2), pp.147–169

Straub, D.W., Gefen, D. and Boudreau, M.C. (2004) *Validation Guidelines for IS Positivist Research.* Communications of the Association for IS. **14**, pp.380–426

Stulz, R.M. (2010) *Six Ways Companies MisManage Risk.* Harvard Business Review

Suler, J. (1996) *The Psychology of Cyberpsace.* [online]. [Accessed 2 September 2015]. Available at: http://users.rider.edu/~suler/psycyber/psycyber.html

Summers, R.C. (1997) *Secure Computing: Threats and Safeguards.* New York: McGraw-Hill

Sunstein, C.R. (2002) *The Paralyzing Principle: Does the Precautionary Principle point us in any helpful direction?* University of Chicago. Regulation. Winter 2002-2003, pp.32-37

Susskind, R. and Susskind, D. (2015) *The Future of the Professions*, Oxford: Oxford University Press, ISBN: 978-0-19-879907-8

Sutherland, Iain (2010) *Skills, Qualifications and Experience - How do we measure these and what will we need in the future?* InfoSec Solutions

Swanson, D. (2006a) *InfoSec, Practical guidance on how to prepare for successful audits.* IT Audit Checklist Series. IT Compliance Institute (www.itcinstitute.com)

Swanson, D. (2006b) *Risk Management, Practical guidance on how to prepare for successful audits.* IT Audit Checklist Series. IT Compliance Institute (www.itcinstitute.com)

Swanson, D. (2011) *IT Security Resources listings.* [online]. [Accessed 8 February 2011]. Available at: http://www.auditnet.org/articles/DSIA201006.htm

Swanson, M. and Guttman, B. (1996) *Generally Accepted Principles and Practices for Securing IT Systems.* NIST (SP 800-14). U.S. Dept. of Commerce: Technology Admin

Swetman, D. and Swetman, R. (2009) *Writing your Dissertation.* Oxford: How To Books Limited

Sybex (2001) *Security Complete.* Authors: Staron, Adams, Lierley. California: Sybex Inc.

Symantec (2007a) *Government Internet Security Threat Report, Trends for January – June 07*

Symantec (2007b) *Have confidence in your IT environment*

Symantec (2009) *Government Internet Security Threat Report, Trends for 2008.* Volume **XIV**

Symantec (2011) *2010 Annual Study: U.S. Cost of a Data Breach - Compliance pressures, cyber attacks targeting sensitive data drive leading IT organizations to respond quickly and pay more.* [online]. with Ponemon Institute. [Accessed 27 March 2011]. Available at: http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf

Symons, C. and Cullen, A. (2008) *Creating A Culture Of Performance And Value.* Forrester Research, Inc.

Taleb, N.N. (2008) *The Black Swan*: *The Impact of the Highly Improbable.* London: Penguin

Talend (2011) *The Butterfly Effect on Data Quality – How small data quality issues can lead to big consequences.* White Paper. Talend Open Integration Solutions

Tarraf, H. (2010) *Literature Review on Corporate Governance and the Recent Financial Crisis.* [online]. [Accessed 15 February 2011]. Available at SSRN: http://ssrn.com/abstract=1731044

Tehan, R. (2012) *Cybersecurity: Authoritative Reports and Resources.* Library of Congress Washington DC Congressional Research Service. [online]. 26 April. [Accessed 17 March 2016]. Available at: https://www.fas.org/sgp/crs/misc/R42507.pdf

Tehan, R. (2013) *Cybersecurity: Authoritative Reports and Resources*. Library of Congress Washington DC Congressional Research Service

The Honeynet Project, (2002) *Know Your Enemy: Revealing the Security Tools, Tactics, and Motives of the Blackhat Community.* Indianapolis: Pearson Education /Addison-Wesley

The Open Group (2011) *Open InfoSec Management Maturity Model (O-ISM3).* Reading: The Open Group. Document Number: C102

The Sun (2010) *Our war secrets £18.87 on eBay.* [online]. [Accessed 8 March 2011]. Available at: http://www.thesun.co.uk/sol/homepage/news/campaigns/our_boys/3222137/Our-war-secrets-1887-on-eBay.html

Thomas, J.P. and Essaaidi, M. (2005) *IA and CompuSec.* Amsterdam. NLD: IOS Press. p.ii

Thomas, M. and Holt, N. (2008) *Building Trust in Critical Systems – BCS Position Statement on Systems that must be Dependable*

Thomas, R. and Walport, M. (2008) *Data Sharing Review Report.* [online]. [Accessed 7 February 2011]. Available at: http://www.justice.gov.uk/reviews/datasharing-intro.htm

Thomson Reuters (2013b) *Regulatory Change Management: The Critical Compliance Competence.* [online]. Accelus. [Accessed 26 April 2015]. Available at: http://accelus.thomsonreuters.com/whitepaper/regulatory-change-management-critical-compliance-competence-0

TNA (undated) *Knowledge and Information Standards and Guidelines.* [online]. [Accessed 17 March 2016]. Available at: http://www.nationalarchives.gov.uk/information-management/policies/publications.htm

Toigo, J.W. (2003) *Disaster Recovery Planning: Preparing for the unthinkable.* 3rd edition. New Jersey: Prentice Hall

Tomorrow's Company (2013) *Tomorrow's Corporate Governance: The boardroom and risk.* [online]. [Accessed 17 March 2016]. Available at: www.tomorrowscorporategovernance.com

Toomey, M. (2009) *The Infonomics Letter – Governance and Management*

Tone at the Top (TATT) (2009a) *A New Level of Audit Committee Involvement.* Issue 44. Florida: Institute of Internal Auditors

TATT (2009ba) *What's on Your (Corporate) Conscience?* Issue 45. Florida: Institute of Internal Auditors

TATT (2010a) *A Culture of Risk.* Issue 46. Florida: Institute of Internal Auditors

TATT (2010b) *We need to talk.* Issue 47. Florida: Institute of Internal Auditors

TATT (2010c) *What GRC could mean for your organization*? Issue 48. Florida: Institute of Internal Auditors

TATT (2010d) *What's your definition of value*? Issue 49. Florida: Institute of Internal Auditors

TATT (2011a) *Soft and Strong: A Best-practice Paradox.* Issue 50. Florida: Institute of Internal Auditors

TATT (2011b) *A View from the Top.* Issue 51. Florida: Institute of Internal Auditors

TATT (2015) *The Tactful Skeptic.* Issue 71. Florida: Institute of Internal Auditors

Tripwire (2011) *Five Mistakes to Avoid in Risk Management and Security*: *Executive Brief.*

Trustwave (2015) *Security Pressures Report*. [online]. [Accessed 25 April 2015]. Available at: https://www2.trustwave.com/security-pressures-report-2015.html

Tsoumas, B. and Gritzalis, D. (2006) *Towards an Ontology-based Security Managemen.* In *Advanced Information Networking and Applications. AINA 2006. 20th International Conference.* **1**(18-20), pp.985,992. doi: 10.1109/AINA.2006.329

Turnbull, S. (1998) *Corporate Charters with Competitive Advantages.* [online]. [Accessed 15 February 2011]. Available at SSRN: http://ssrn.com/abstract=10570 or doi:10.2139/ssrn.10570

Turnbull, N. (1999) *Internal Control: Guidance for Directors on the Combined Code.* ICAEW

Turnbull, S. (2009a) *Why 'Best' Corporate Governance Practices are Unethical and Less Competitive.* BUSINESS ETHICS: DECISION-MAKING FOR PERSONAL INTEGRITY & SOCIAL RESPONSIBILITY, 2E, L. Hartman, J. DesJardins, (eds.). Burr Ridge, IL: McGraw-Hill. [online]. [Accessed 3 February 2011]. Available at SSRN: http://ssrn.com/abstract=1260047

Turnbull, S. (2009b) Chapter 5 *What's Wrong with Corporate Governance 'Best' Practices*? [online]. In *CORPORATE GOVERNANCE*, H. Kent Baker, Ronald Anderson, (eds.), New York: John Wiley & Sons Inc. [Accessed 3 February 2011]. Available at SSRN: http://ssrn.com/abstract=1506954

Turnbull, S. (2008) *Mitigating the Exposure of Corporate Boards to Risk and Unethical Conflicts.* [online]. [Accessed 15 February 2011]. Available at: http://ssrn.com/abstract=1106792

UCISA (2005) *InfoSec Toolkit.* [online]. 3rd edition, UCISA

UK Cabinet Office (1999b) *Delivery if Public Services, 24 Hours a Day, Seven Days a Week (24 x 7).* October-December

UK Cabinet Office (2000) *Implementing E-Government – Guidelines for Local Government*. April 2000, Department of the Environment, Transport and Regions (DETR), the Local Government Association (LGA) and the Improvement and Development Agency (IDeA)

UK Cabinet Office (2001) *Open all hours, Service hours at times to suit, citizens first – a report on extended service hours.* Modernising Government

UK Cabinet Office (2002b) *Privacy and Data Sharing.* Performance and Innovation Unit

UK Cabinet Office (2003) *Draft Civil Contingencies Bill*

UK Cabinet Office (2004b) *e-Government Interoperability Framework, Technical Standards Catalogue.* Version 6.1. e-Government Unit

UK Cabinet Office (2005a) *Computer Misuse Act 1990* (Amendment) Bill issued

UK Cabinet Office (2005b) *e-Government Interoperability Framework.* Version 6.1. e-Government Unit

UK Cabinet Office (2007b) *Government response to Power of Information task force.* [online]. [Accessed 2 September 2015]. Available at: http://www.official-documents.gov.uk/document/cm71/7157/7157.asp

UK Cabinet Office (2008c) *National Risk Register*

UK Cabinet Office (2009h) *2010 Cabinet Office Information Risk Report: HMG IA Maturity Model Supported Self-Assessment*

UK Cabinet Office (2010d) *Cabinet Office Structural Reform Plan*

UK Cabinet Office (2010e) *Deed relating to The Participation in the Public Sector Network as a Government Conveyance Network Service Provider*

UK Cabinet Office (2011f) *Corporate governance in central government departments: Code of good practice 2011 – Guidance Note.* with HM Treasury. London: Whitehall

UK Cabinet Office (2013) *Government Security Classifications, April 2014*, Version 1.0, October 2013

UK Centre for Protection of National Infrastructure (CPNI) (undated, a) *CPNI A good practice guide on pre employment screening.* [online]. 5th edition. [Accessed 1 March 2015]. Available at: http://www.cpni.gov.uk/documents/publications/2015/pre-employment%20screening%20edition%205%20-%20final.pdf?epslanguage=en-gb

UK CPNI (undated, b) CPNI Physical Security measures

UK CPNI (2013) *Influencing Company Boards.* CPNI. [online]. [Accessed 26 April 2015]. Available at: https://www.cpni.gov.uk/documents/publications/2013/2013009-influencing_company_boards.pdf?epslanguage=en-gb

UK CESG (1997) *Protecting Government Connections to the Internet.* CESG InfoSec Memorandum No. 13. Cheltenham: CESG

UK CESG (undated) *Protection Profiles.* Cheltenham: CESG

UK CESG (2005a) HMG InfoSecStandard No. 2 *Risk management and accreditation of information systems.* As published by NISCC. Issue 1.0. Cheltenham: CESG – renamed to IA. [online]. [Accessed 1 March 2015]. See http://en.wikipedia.org/wiki/HMG_Infosec_Standard_No.1

UK CESG (2005b) *InfoSec Memorandum 28 – Performance and Assurance Standards for Biometric Systems Contributing to multi-element identification and authentication'.* Issue 1.0. Cheltenham: CESG

UK CESG (2008) *CESG IA Memorandum 26 – Passwords for identification and authentication.* Issue 4.0. Cheltenham: CESG

UK CESG (2009a) *HMG IA Maturity Model and Assessment Criteria.* CESG and Cabinet Office. V3.0

UK CESG (2009b) *Busy Reader Guide Managing the risks from online social networking.* Version 1.0. National Technical Authority for IA. Cheltenham: CESG

UK CESG (2009c) *Good Practice Guide 13 – Protective Monitoring for HMG ICT Systems.* Issue 1.3. Cheltenham: CESG

UK CESG (2009d) *Good Practice Guide 18 - Forensic Readiness.* Issue 1.0. Cheltenham: CESG

UK CESG (2009i) *Good Practice Guide 6 - Outsourcing and Offshoring: Managing the Security Risks.* Issue 2.0. Cheltenham: CESG

UK CESG (2010b) *Biometrics.* Cheltenham: CESG

UK Conservatives (2010a) *A Resilient Nation: National Security Green Paper.* Policy Green Paper No. 13. London: Alan Mabbutt

UK Conservatives (2010b) *Conservative Technology Manifesto.* London: Alan Mabbutt

UK DEGW and OGC (2008) *Working beyond walls: The government workplace as an agent of change.* With Bell, A., Graham, R., Hardy, B., Harrison, Hutton, L., A., Stansall, P. and White, A.

UK Department for Communities and Local Government (DCLG) (2011) *Code of recommended practice for local authorities on data transparency Consultation*

UK Department for Education and Skills (2003) *Towards a Unified e-Learning Strategy.* Consultation Document

UK Department of Business, Innovation & Skills (BIS) (2005) *Hampton Review – Reducing administrative burdens: effective inspection and enforcement*. [online]. Sir Philip Hampton. [Accessed 8 March 2011]. Available at: http://www.bis.gov.uk/policies/better-regulation/improving-regulatory-delivery-assessing--our-regulatory-system

UK BIS (2010) *InfoSec Breaches Survey, 2010.* PriceWaterhouseCoopers

UK Department of Trade and Industry (DTI) (2004) *DTI InfoSec Breaches Survey 2004.* Technical Report. PricewaterhouseCoopers

UK DTI (2006) *DTI InfoSec Breaches Survey 2006.* PriceWaterhouseCoopers

UK DTLR (2002a) *e-gov@local, Towards a national strategy for local e-government, A consultation paper. Summary*

UK DTLR (2002b) *e-gov@local, Towards a national strategy for local e-government, A consultation paper. Main Document*

UK eGov (2003) *the local e-government standards body, The National Standards Authority for Local e-Government*

UK eGov (2005) *e-GIF Registration & Authentication framework*. [online]. The e-GIF Accreditation Authority. [Accessed 1 March 2015]. Available at: http://systems.hscic.gov.uk/rasmartcards/documents/raegif.pdf

UK HMG (2000) *Regulation of Investigatory Powers Act.* [Act of Parliament]. [online]. [Accessed 6 February 2011]. Available at: http://www.legislation.gov.uk/ukpga/2000/23/contents

UK HMG (2005) *eAccessibility of public sector services in the European Union, Executive briefing*

UK HMG (2007a) *Government IT Profession CIO Toolkit.* [online]. cited in Grafton, A-M., (undated) *Embedding IT Professionalism in Your Organisation.* Presentation *http://bcs.org/upload/pdf/government-profession-amgrafton.pdf see also https://www.gov.uk/government/organisations/civil-service-government-it-profession/about*

UK HMG (2007b) *Explanatory Memorandum to The Regulation of Investigatory Powers (Investigation of Protected Electronic Information: Code of Practice).* Order 2007

UK HMG (2007c) *Personal Internet Security, The Government Reply to the Fifth Report from the House of Lords Science and Technology Committee Session 2006-07.* HL Paper 165. Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty

UK HMG (2010b) *National Security Risk Assessment fact sheet*

UK HMG (2011a) *Government Response to the Intelligence and Security Committee's Annual Report 2010-2011.* Presented to Parliament by the Prime Minister by Command of Her Majesty. Cm 8168. London: HMSO

UK HMG (2016) *Prospectus: Introducing the National Cyber Security Centre*. [Last accessed 6 March 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf

UK HM Treasury (2009a) *Putting the Frontline First: Smarter Government.* Cm. 7753. London: HMSO. pp.22-25. [online]. [Accessed 13 November 2010]. Available at: http://www.hmg.gov.uk/media/52788/smarter-government-final.pdf

UK HM Treasury (2009b) *Operational Efficiency Programme.* [online]. [Accessed 4 May 2010]. Available at: http://www.hm-treasury.gov.uk/vfm_operational_efficiency.htm

UK Home Office (2004*) The police recording of computer crime.* Home Office Development and Practice Report

UK House of Lords (2007) *Personal Internet Security Volume I: Report, House of Lords Science and Technology Committee 5th Report of Session 2006-07.* HL Paper 165-I

UK House of Lords (2008) *Personal Internet Security: Follow Up, House of Lords Science and Technology Committee.* 4th Report of Session 2007-08

UK House of Lords (2009) *Surveillance: Citizens and the State,* Constitution Committee. London: House of Lords Constitution Committee. [online]. [Accessed 17 March 2016]. Available at: http://www.publications.parliament.uk/pa/ld200809/ldselect/ldconst/18/1802.htm

UK House of Lords (2010) *Protecting Europe against large-scale cyber-attacks.* HL Paper 68. European Union Committee, London: HMSO

UK Identity & Passport Service (2010) *Draft Identity Rights Charter for consideration by the IPS.* From the IPS Expert Panel. Draft 10

UK Information Commissioner's Office (ICO) (2007a) *Home Affairs Committee Inquiry into "The Surveillance Society*?". Evidence Submitted by the Information Commissioner. Cheshire: ICO

UK ICO (2007b) *Framework code of practice for sharing personal information.* Cheshire: ICO

UK ICO (2007c) *Surveillance Society: Turning debate into action.* Conference Papers. [online]. 11 December [Accessed 5 November 2010]. Available at: http://www.ico.gov.uk/news/current_topics/2007.aspx. See also: http://www.ico.gov.uk/Home/news/current_topics/Surveillance_society_conference.aspx

UK ICO (undated) *Processing personal data fairly and lawfully.* [online]. [Accessed 17 March 2016]. Available at: https://ico.org.uk/for-organisations/guide-to-data-protection/principle-1-fair-and-lawful/

UK ICO (2010a) *The Privacy Dividend: the business case for investing in proactive privacy protection*

UK ICO (2010b) *Information Commissioner's report to Parliament on the state of surveillance*. Update to the *House of Lords 2006, Report: Surveillance, Citizens and the State.* [online]. [Accessed 1 March 2015]. Available at https://ico.org.uk/media/about-the-ico/documents/1042386/surveillance-report-for-home-select-committee.pdf

UK ICO (2011) *Promoting openness by public bodies and data privacy for individuals – An information rights strategy for the ICO.* Version 1.0

UK LGA (2000) *Targets for Local Government*

UK Local eGovernment Standards Body (2005) *Prospectus for operating an e-standards service*

UK Local Government Information Unit (LGiU) (2002) *The abc of e-government.* [online]. [Last accessed 24 March 2016]. Available at: http://www.lgiu.org.uk

UK LGITU (2009) *Connecting the Public Sector – Executive Summary - Safeguarding citizen data in an unsafe world.* Informed Publications Ltd. [online]. [Accessed 18 February 2011]. Available at: http://issuu.com/informed/docs/connectingpublicsectorexecsummnov09

UK National Infrastructure Security Co-Ordination Centre (NISCC) (2002) *The Security of 802.11 Wireless Networks.* Technical Note 04/02

UK NISCC (2004) *Using External Security Specialists. Good Practice Guide.* NISC

UK NISCC (2005) *Protecting Data Centres.* Policy and Best Practice 00759 Guide

UK OCSIA (2010) *Office of Cyber Security and IA*. [online]. [Accessed 7 February 2011]. Available at: http://www.cabinetoffice.gov.uk/content/office-cyber-security-and-information-assurance-ocsia

UK Office of the Deputy Prime Minister (ODPM) (2005a) *Two Years On, The national strategy for local e-government*

UK ODPM (2005b) *Local e-Government Partnerships*

UK ODPM (2005c) *Priority Service & National Strategy transformation outcomes for local e-government in December 2005*

UK Office of Fair Trading (OFT) (2006) *Competition Commission and Office of Fair Trading – Commercial Use of Information*

UK Office of Government Commerce (OGC) (2003) *Successful Delivery Toolkit*, Version 4.02

UK Office of Public Sector Information (OPSI) (1998) *Data Protection Act 1998*. [Act of Parliament]. London: HMSO. [online]. [Accessed 23 March 2016]. Available at: http://www.legislation.gov.uk/ukpga/1998/29/contents

UK OPSI (2000) *Freedom of Information Act 2000.* [Act of Parliament]. [online]. [Accessed 17 March 2016]. Available at: http://www.legislation.gov.uk/ukpga/2000/36/contents

UK OPSI (2001) *Convention on Cybercrime. CM7862.* Original legislation. Council of Europe. Budapest. [online]. [Accessed 23 March 2016]. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/238440/7862.pdf

UK OPSI (2004) *Environmental Information Regulations 2004/3391.* [Act of Parliament]. [online]. [Accessed 17 March 2016]. Available at: http://www.legislation.gov.uk/uksi/2004/3391/contents/made

UK Parliamentary Office of Science and Technology (POST) (2003) *Government IT Projects*

UK PITCOM (2008) "*Who can access my data?" paper.* Various resources from the Parliamentary IT Committee. [online]. [Accessed 6 February 2011]. Available at: http://www.pitcom.org.uk/modules.php?op=modload&name=News&file=index&catid=&topic=5

Urquhart, C., Lehmann, H. and Myers, M.D. (2010) Putting the 'theory' back into grounded theory: guidelines for grounded theory studies in IS. *IS Journal.* **20**(4), pp.357-381

US Committee on National Security Systems *(*CNSS) (2004a) *CNSS Instruction 4012 National IA Training Standard for Senior System Managers*. [online]. [Accessed 1 March 2015]. Available at https://www.ecs.csus.edu/csc/iac/cnssi_4012.pdf

US CNSS (2004b) *CNSS Advisory Memorandum for IA - Security Through Product Diversity* (1/04)

US CNSS (2005a) *CNSS Advisory Memorandum on the Retirement of Data Encryption Standard (DES) Based Cryptography to Protect National Security Systems (02/04)*

US CNSS (2005a) *CNSS Instruction 4016: National IA Training Standard for Risk Analysts*

US CNSS (2006) *CNSS Directive No. 500: IA Education, Training, and Awareness*

US CNSS (2007) *CNSS Directive 048-0:7 National IA Approach to Incident Management (IM)*

US CNSS (2009) *CNSS Directive Policy No. 22: IA Risk Management Policy for National Security Systems (NSS)*

US CNSS (2010) *CNSS Directive No. 24: Policy on Assured Information Sharing (AIS) for NSS*

US Corporate Governance Task Force (2004) *National Cyber Security Summit Task Force: Corporate Governance Report*

US Critical Infrastructure Assurance Office (2000) *Practices for Securing Critical Information Assets.* Washington: CIAO

US Critical Infrastructure Protection Board (2002) *The President's National Strategy to Secure Cyberspace.* White House

US Department of Defense (DoD) (1997) *DOD Instruction 5200.40:* DoD Information Technology Security Certification and Accreditation Process (DITSCAP)

US DoD (2000) *DoD 8510.1M, IT Security Certification and Accreditation Process (DITSCAP*) Application Manual

US DoD (2002a) *DOD Directive 8000.1: Management of Information Resources and IT*

US DoD (2002b) *DoD Directive 8500.1: IA Manual, DoD Directive 8500.1-M* (when effective)

US DoD (2003) *DoD Instruction 8500.2: IA Implementation*

US DoD (2005) *Directive 8570.01-M - IA Training, Certification and Workforce Management.* [online]. Written up in *IA Workforce Improvement Program.* [Accessed 1 March 2015]. Available at: http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf

US DoD (2007) *DoD Directive: IA.* NUMBER 8500.01E

US DoD (2008) *DoD Instruction DoDI 8500-2 IA Control Checklist - MAC 3-Public Version 1.* Release 1.4

US Department of Homeland Security (DHS) (1984) *Executive Order 12472 - Assignment of National Security and Emergency Preparedness Telecommunications Functions.* As amended by US Executive Order 12472 (2012). *Assignment of National Security and Emergency Preparedness Communications Functions.* [online]. [Accessed 1 March 2015]. Available at: http://www.whitehouse.gov/the-press-office/2012/07/06/executive-order-assignment-national-security-and-emergency-preparedness-

US DHS (2001) *Executive Order 13231, Critical Infrastructure Protection in the Information Age.* [online]. As amended by *EO 13286: Transfer of Certain Functions to the Secretary of Homeland Security.* [Accessed 1 March 2015]. Available at https://www.dhs.gov/xlibrary/assets/executive-order-13231-dated-2001-10-16-initial.pdf and http://fas.org/irp/offdocs/eo/eo-13286.htm respectively

UK DHS Office (2010) *National Strategy for Trusted Identities in Cyberspace Creating Options for Enhanced Online Security and Privacy*. [online]. [Accessed 23 March 2016]. Available at: https://www.dhs.gov/xlibrary/assets/ns_tic.pdf

US DHS (2013) *Executive Order 13636 - Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) on Critical Infrastructure Security and Resilience*. [online]. [Accessed 1 March 2015]. Available at http://www.dhs.gov/publication/fact-sheet-eo-13636-improving-critical-infrastructure-cybersecurity-and-ppd-21-critical

US Government Accountability Office (GAO) (1998) *Accounting and IM Division, Executive Guide InfoSec Management, Learning from Leading Organisations.* [online]. [Accessed 21 January 2011]. Available at: http://www.gao.gov/archive/1998/ai98068.pdf

US GAO (2009) *Federal Information System Controls Audit Manual (FISCAM).* GAO-09-232G

US GAO (2016) Federal Chief Information Security Officers: Opportunities Exist to Improve Roles and Address Challenges to Authority, August 2016, [Last accessed 6 March 2017]. Available at: http://www.gao.gov/products/GAO-16-686

US Government (2010) *Cyber Space Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure*

US Government Reform Committee (2004) *Corporate InfoSec Working Group, Report of the Best Practices and Metrics Teams,* United States House of Representatives

US National Computer Security Center (NCSC) (1987) TG-005: *Trusted Network Interpretation (TNI).* [online]. [Accessed 1 March 2015]. Available at: http://fas.org/irp/nsa/rainbow/tg005.htm

US NCSC (1992) *NCSC-TG-027: A Guide To Understanding Information System Security Officer Responsibilities for Automated Information Systems.* Version 1, May

US NCSC (1994) *NCSC-TG-029: Introduction to Certification and Accreditation.* Version 1, January

US NIST (1996) *NIST SP 800-14: Generally Accepted Principles and Practices for Securing Information Technology Systems.* [online]. [Accessed 5 February 2011]. Available at: http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf

US NIST (1998a) *NIST SP 800-16: ITSec Training Requirements: A Role-and Performance-based Model*

US NIST (1998b) *NIST SP 800-18: Guide for Development of Security Plans for IT Systems* B-1 ANNEX B to CNSSI No. 4012B- 2 ANNEX B to CNSSI No. 4012

US NIST (2001a) *NIST SP 800-26: Security Self-Assessment Guide for IT Systems.* Marianne Swanson

US NIST (2003) *NIST SP 800-64: Security Considerations in the IS Development Life Cycle*

US NIST (2004b) *NIST SP 800-27: Engineering Principles for ITSec (A Baseline for Achieving Security).* Revision A

US NIST (2006a) *NIST SP 800-18: Guide for Developing Security Plans for Federal IS.* Revision 1

US NIST (2006b) *NIST SP 800-100: InfoSec Handbook: A Guide for Managers.* [online]. October 2006. [Accessed 17 March 2016]. Available at: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

US NIST (2006c) *NIST SP 800-53: Recommended Security Controls for Federal IS.* Revision 1. December

US NIST (2006d) NIST SP 800-63: *Electronic Authentication Guideline.* April 2006

US NIST (2007a) *NIST SP 800-97: Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i*

US NIST (2007b) *NIST SP 800-98: Guidelines for Securing Radio Frequency Identification (RFID) Systems*

US NIST (2007c) *NIST SP 800-54: Border Gateway Protocol Security*

US NIST (2008a) *NIST SP 800-61: Computer Security Incident Handling Guide.* [online]. [Accessed 27 March 2011]. Available at: http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

US NIST (2008b) *NIST SP 800-123: Guide to General Server Security* (Draft)

US NIST (2008c) *NIST SP 800-113: Guide to SSL VPNs*

US NIST (2008d) *NIST SP 800-124: Guidelines on Cell Phone and PDA Security* (Draft)

US NIST (2009a) *NIST SP 800-46: Guide to Enterprise Telework and Remote Access Security.* Revision 1

US NIST (2009b) *NIST SP 800-53: Recommended Security Controls for Federal IS and Organizations*

US NIST (2009c) *NIST SP 800-41: Guidelines on Firewalls and Firewall Policy*. Revision 1

US NIST (2009d) *NISTIR 7621: Small Business InfoSec: The Fundamentals*

US NIST (2010a) *NIST SP 800-53: Recommended Security Controls for Federal IS and Organizations.* Revision 3

US NIST (2010b) *Federal Enterprise Architecture Security and Privacy Profile.* Version 3.0

US NIST (2010c) *NIST SP 800-137: InfoSec Continuous Monitoring for Federal IS and Organizations*

US NIST (2011a) *NIST SP 800-125: Guide to Security for Full Virtualization Technologies*

US NIST (2011b) *NIST SP 800-39: Managing InfoSec Risk.* [online]. [Accessed 17 August 2015]. Available at: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

US NIST (2011c) *NIST SP 800-144: Guidelines on Security and Privacy in Public Cloud Computing.* Draft, January; full version, December

US NIST (2011d) *NIST SP 800-145: The NIST Definition of Cloud Computing (DRAFT)*

US NIST (2011e) *NIST SP 800-30: Guide for Conducting Risk Assessments.* Initial Public Draft

US NIST (2011f) *NIST SP 800-144: Guidelines of Security and Privacy in Public Cloud Computing*

US NIST (2011g) *NIST SP 800-63-1*, *Electronic Authentication Guideline.* [online]. [Accessed 1 March 2015]. Available at: http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf

US NIST (2012a) *Security and Privacy Controls for Federal IS and Organizations.* Initial Public Draft

US NIST (2012b) *Cloud Computing Synopsis and Recommendations*

US NIST (2013) *NIST SP 800-63-2, Electronic Authentication Guideline.* [Accessed 1 March 2015]. Available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-2.pdf

US NIST (2013) *NIST SP 800-53, Security and Privacy Controls for Federal IS and Organizations.* [online]. [Accessed 21 June 2015]. Available at http://dx.doi.org/10.6028/NIST.SP.800-53r4

US NIST (2015) *NISTIR 8062. Privacy Risk Management for Federal Information Systems.* Draft

US NIST (2016) *NIST SP 800-150, Guide to Cyber Threat Information Sharing*. [Last accessed 14 March 2017]. Available at: http://csrc.nist.gov/publications/drafts/800-150/sp800_150_second_draft.pdf

US NIST (2016) *NIST SP 800-160, Systems Security Engineering: An Integrated Approach to Building Trustworthy Resilient Systems*. May 2016. Draft. [Accessed 9 October 2016]. Available at: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf

US NIST (2016) *NIST SP 800-181, NICE Cybersecurity Workforce Framework (NCWF).* [Last accessed 14 March 2017]. Available at: http://csrc.nist.gov/publications/drafts/800-181/sp800_181_draft.pdf

US NIST (2016) *NIST SP 800-184, Guide for Cybersecurity Event Recovery*. [Last accessed 14 March 2017]. Available at: http://csrc.nist.gov/publications/drafts/800-184/sp800_184_draft.pdf

US NIST FIPS (1974) *Federal Information Processing Standards Publication (FIPS) Publication 31, Guidelines for Automatic Data Processing Physical Security and Risk Management*

US NIST FIPS (1981) *Federal Information Processing Standards Publication (FIPS) 87, Guidelines for ADP Contingency Planning*

US NIST FIPS (1983) *Federal Information Processing Standards Publication (FIPS) Publication 102, Guideline for Computer Security Certification and Accreditation*

US NIST FIPS (1993) *Federal Information Processing Standards Publication (FIPS) Publication 65, Guideline for Automatic Data Processing Risk Analysis*

US NIST FIPS 140-2 (2002) *Security Requirements for Cryptographic Modules*

US NIST FIPS 199 (2004) *Standards for Security Categorization of Federal Information and IS*

US NIST FIPS 200 (2006) *Minimum Security Requirements for Federal Information and IS*

US National Security Agency (undated) *Defense in Depth: A practical strategy for achieving IA in today's highly networked environments.* [online]. [Accessed 5 February 2011]. Available at: http://www.nsa.gov/ia/_files/support/defenseindepth.pdf

US National Security Council (1992) *National Policy for the Security of National Security Telecommunications and IS.* NSD 42. [online]. [Accessed 1 March 2015]. Available at: http://fas.org/irp/offdocs/nsd/nsd_42.htm

US NSTIC (2010) *National Strategy for Trusted Identities in Cyberspace Creating Options for Enhanced Online Security and Privacy* (DRAFT)

US NSTISSD (1992) *NSTISSD 501: National Training Program for IS Security (INFOSEC) Professionals*

US Office of Management and Budget (OMB) (2000a) *OMB Circular No. A-130: Revised (Transmittal Memorandum No. 4), Management of Federal Information Resources*. 30. November

US OMB (2000b) *OMB Memorandum M-00-07: Incorporating and Funding Security in IS Investments*

US OMB (2001a) *OMB Memorandum M-01-08: Guidance on Implementing the Government InfoSec Reform Act*

US OMB (2001b) *OMB Memorandum M-01-24: Reporting Instructions for the Government InfoSec Reform Act*

US OMB (2001c) *OMB Memorandum M-02-0: Guidance for Preparing and Submitting Security Plans of Action and Milestones*

US Office Of Personnel Management (OPM) (2004) *InfoSec Responsibilities for Employees who manage or use Federal IS,* Code of Federal Regulations, 5 C.F.R. §903 et seq.. [online]. June. [original wording *Employees Responsible for the Management or Use of Federal Computer Systems*, updated 2014]. Linked to Executive Order 12866. [Accessed 17 March 2016]. Available at https://www.federalregister.gov/articles/2003/09/04/03-22487/employees-responsible-for-the-management-or-use-of-federal-computer-systems and http://csrc.nist.gov/drivers/documents/OPM-June2004-updated-sectrainaware.html

Vaishnavi, V. and Kuechler, B. (2004) *Design Science Research in IS.* Last updated 15 November 2015. Retrieved from: http://desrist.org/desrist/content/design-science-research-in-information-systems.pdf

Valeri, L. (2000) Securing Internet society: Toward an international regime for information assurance. *Studies in Conflict and Terrorism*, **23**(2), pp.129-146.

Valeri, L. (2002) *Dot.com versus dot.gov : states, international businesses and an international regime for information assurance.* (Doctoral dissertation, King's College London, University of London)

Valeri, L., Rathmell A. and Daman, S. (2002) *Information Risk: Implications for the Financial Sector.* RAND Europe

Van Maanen, J. and Barley, S.R. (1984) Occupational communities: Culture and control in organizations. *Research in Organizational Behavior*, **6**, pp.287-365.

Verkaik, R. (2009) *Trust in Whitehall falls to a new low.* Law Editor. [online]. [Accessed 5 February 2011]. Available at: http://www.independent.co.uk/news/uk/politics/trust-in-whitehall-falls-to-a-new-low-1671330.html

Vicente, P. and da Silva, M.M. (2011) *A Conceptual Model for Integrated Governance, Risk and Compliance*, in *Advanced Information Systems Engineering.* pp.199-213. Berlin Heidelberg: Springer

Vicente, P. (2011) *A Reference Architecture for Integrated Governance, Risk and Compliance.* [online]. [Accessed 16 March 2016]. Available at: https://fenix.tecnico.ulisboa.pt/downloadFile/395143146329/disserta%C3%A7%C3%A3o.pdf

Vormetric (2015) *2015 Insider Threat Report.* Global Edition. [online]. [Accessed 25 April 2015]. Available at: http://www.vormetric.com/campaigns/insiderthreat/2015/

Walsham, G. (1993) *Interpreting IS in Organizations.* Chichester: Wiley

Walsham, G. (1995a) Interpretive case studies in IS research: nature and method. *European Journal of IS.* **4**, pp.74–81

Walsham, G. (1995b) The Emergence of Interpretivism in IS Research. *IS.* **6**(4), pp.376–394

Wall, D.S. (2001) *Crime and the Internet.* London: Routledge

Wall, D.S. (2007) *Cybercrime: The Transformation of Crime in the Information Age.* Cambridge: Polity Press

Ward, J. and Peppard, J. (2002) *Strategic Planning for IS.* 3rd edition. Chichester: John Wiley & Sons

Warren, P. and Streeter, M. (2005) *cyber alert, How the World is Under Attack from a New Form of Crime.* London: Vision Paperbacks

Wash, R. (2010) *Folk Models of Home Computer Security.* Michigan State University

Watson, D. and Floridi, L. (2016) Crowdsourced science: sociotechnical epistemology in the e-research paradigm. *Synthese*, pp.1-24. [Accessed 18 February 2017]. Available at: http://link.springer.com/article/10.1007/s11229-016-1238-2

Weisman, R. (2011) *Better Understanding Electronically Stored Information – Know what you have, How long it needs to be kept and how best to store it.* In Processor.com, p.30

Welch, D., Ragsdale, D. and Schepens, W. (2002) *Training for IA.* IEEE. *Computer.* **35**(4), pp.30-37

White House (2010) *United States Cyberspace review documents resource.* [online]. [Accessed 6 February 2011]. Available at: http://www.whitehouse.gov/cyberreview/documents

Whyte, W.H. (1956) *The Organization Man.* Pennsylvania: University of Pennsylvania Press. Reprinted 2002

Widup, S. (2010) *The Leaking Vault - Five Years of Data Breaches.* Digital Forensics Association

Wilensky, H. (1964) The professionalization of everyone? *American Journal of Sociology*, **70**(2), pp.137-158

Willcocks, L.P. and Mingers, J. (2004) *Social theory and philosophy for IS.* John Wiley & Sons Ltd

Winkler, I. (2005) *Spies Among Us.* Indianapolis: Wiley Publishing

Winnett, R. (2008) *Home Office loses confidential data on all UK prisoners,* Deputy Political Editor. [online]. [Accessed 6 February 2011]. Available at: http://tinyurl.com/68pre6 and http://www.telegraph.co.uk/news/uknews/law-and-order/2598204/Home-Office-loses-confidential-data-on-all-UK-prisoners.html

Woerner, R. (2010) The Real Risk Equation. *InfoSecurity Magazine.* pp.8-9

Wolf, D.G. (2003) *Statement by NSA's Director of IA before the House Select Committee on Homeland Security,* US House of Representatives

World Economic Forum (WEF) (2012a) *Partnering for Cyber Resilience: Risk and Responsibility in a Hyperconnected World – Principles and Guidelines*, REF 270912

WEF (2012b) *Global Risks 2012 Seventh Edition: An Initiative of the Risk Response Network*, Insight Report, REF: 030112

WEF (2014) *Insight Report: Risk and Responsibility in a Hyperconnected World*

WEF (2015) *Insight Report: The Global Information Technology Report: ICTs for Inclusive Growth.* [online]. [Accessed 24 March 2016]. Available at: www.weforum.org/gitr

WEF (2016) *The Global Risks Report 2016*. 11th Edition

Wu, T. (2011) *The Rise and Fall of Information Empires.* RSA Lecture. [online]. [Accessed 24 April 2011]. Available at: http://www.thersa.org/events/audio-and-past-events/2011/the-rise-and-fall-of-information-empires

Yarwood-Ross, L. (2014) *Engaging with extant Literature in Grounded Theory: A contentious issue.* RCN research. [online]. [Last acessed 3 May 2015]. Available at: http://www.rcn.org.uk/__data/assets/pdf_file/0008/569213/2014_RCN_research_4.5.1.pdf

Yates, J. and Murphy, C.N. (2007) *Coordinating International Standards: The Formation of the ISO.* MIT Sloan Working Paper 4638-07. MIT Sloan School of Management

Yates, J. and Murphy, C.N. (2008) *Charles Le Maistre: Entrepreneur in International Standardisation.* [online]. [Accessed 28 August 2015]. Available at: http://jyates.scripts.mit.edu/docs/Yates%20Murphy%20%20Histoire%20et%20Entreprise%20submitted.pdf

Zander, R.S and Zander, B. (2000) *The Art of the Possibility.* London: Penguin

Zittrain, J. (2008) *The Future of the Internet and how to stop it.* London: Penguin

Part 4b - Appendices

This section contains:

Appendix I: Original Papers etc.

- *Original Papers*
- *MSc in IG Course Curriculum*
- *Annual University Posters*
- *Survey Questionnaires*
- *Research Demographics*
- *Survey Memos*
- *IA Search methodology used*
- *Other IA Information Sources*
- *Related Standards and Best Practice Resources*
- *IA Definitions*

Appendix II

- *Public Sector Case Study [CS1]*
- *Private Sector Case Study [CS2]*

Appendix III

- *IA Chronology*

10 APPENDIX I: ORIGINAL PAPERS etc.

10.1 List of Original Papers Prepared

1. Simmons (2008) [**book cover below**]
2. Simmons (2009) in Trim and Caravelli (2009) - *A Journey Towards Resilience: Lessons from the British Experience*, pp.131-148 [**book cover below**]
3. Simmons (2011) *MSc IG* – Curriculum [**below**]
4. Simmons (2012a) [**book cover below**]
5. Simmons (2015a) [**book cover below**]

The following articles are included:

- ✓ Simmons (2012b) ***[below]***
- ✓ Simmons (2015b) ***[below]***

The following Posters are represented:

- ✓ 2011 [**below**]
- ✓ 2013 [**below**]
- ✓ 2014 [**below**]
- ✓ 2015 [**below**]

The following Questionnaires are represented:

- ✓ IAAC Review Questionnaire [**below**]
- ✓ Private Sector Review Questionnaire [**below**]

10.2 Presentations Delivered 2009-2017

1. Tackling the barriers to achieving best practice in IA in the UK Public Sector, ENISA Conference, London, 15 May 2009;
2. Tackling the barriers to achieving best practice in IA in the UK Public Sector, ARCS Conference, Oxford, 17 June 2009;
3. Tackling the barriers to achieving best practice in IA in the UK Public Sector, ARCS Workshop, Oxford, 1 June 2010*;*
4. IA in the UK Public Sector: Tackling the barriers to achieving best practice, BCS IRMA, London, 14 December 2010*;*
5. Addressing the Human Factors, Webinar presentation, November 2011;
6. Professionalism and IA, BCS Gloucestershire, 17 January 2012;
7. IA in the UK Public Sector: Tackling barriers to achieving best practices, an update, BCS IRMA, London, 14 March 2012;
8. Armed Forces Communications and Electronics Association (AFCEA) IA: are we sure what it means and why we are doing it?, Cheltenham, Thursday 10 January 2013;
9. Cyber Schmyber: The Relevance of Principles, presentation at BCS SecureSouthWest, 25 March 2013, London – slides available at: http://www.securesouthwest.com/presentations/SSW2/HPEnterpriseServices.pdf;
10. Transparency vs. Compliance, presented at Socitm SouthWest Conference on the topic of, 21 June 2013;
11. The Skills Deficit: Is it Real?, presentation at IISP/Crest Congress, 19 March 2014, London;
12. Attended The Cyber Dimension of Global Security Challenges, Nigel Jones Senior Research Fellow and Director Cyber Masters Programme Cranfield University at the Defence Academy, 12 June 2014, Cheltenham;
13. Systems, Synthesis and Synergy – where SCIT meets FoSS - presentation at Systems, Synthesis and Synergy, The Faculty of Social Sciences PhD Research conference 2014, Monday 30th June 2014, University of Wolverhampton;
14. Securing an organisation with Global Reach, presentation at Cranfield CyberSecurity Conference, Swindon, 21 October 2014;
15. Cyber Schmyber, presentation at Global Institute of Cyber, Security and Intelligence (GICIS) CyberSecurity Intelligence (CSI) launch event, London, 21 January 2015;
16. Making Friends with Internal Audit at ISACA Ireland Conference 2015 – Trust, Security, Agility, 23 October 2015, Available at: http://www.isaca.org/chapters5/Ireland/conference/pages/Agenda.aspx;

17. i3GRC – what's that all about then, eh?! Keynote Presentation at PRISM International Conference, Barcelona, 28 October 2015, Available at: http://www.prismintl.org/News-Press/PRISM-Press-Releases/prism-2015-europe-conf-barcelona.html;
18. Cyber threats: hiding in plain sight, at ESRD 2015 – European Security Research: The Next Wave, 4 November 2015, Available at: http://www.esrdublin2015.eu/;
19. There is nothing new under the sun, Data Protection Day presentation, Irish Computer Society, 28th January 2016;
20. Cyber credibility crisis, BCS: University of Worcester, 4th April 2017;
21. Cyber credibility crisis, BCS: London – Information Risk Management & Assurance (IRMA) Specialist Group, 11th April 2017;
22. Cyber credibility crisis, AFCEA: Cheltenham, 11th May 2017;
23. Terminology and Professionalism, BCS: London - Safe Security Research Day, 31st October 2017.

10.3 MSc in Information Governance – Curriculum Course flyer 2011

Information Governance

"Information Governance" (IG) is the set of multi-disciplinary structures, policies, procedures, processes and controls implemented to manage information on all media in such a way that it supports an organisation's immediate and future regulatory, legal, risk, environmental and operational requirements. Central to IG is an understanding of the journey from IT Security, through Information Security (InfoSec), to Information Assurance (IA) – all of which are about maturing to a position of being able to demonstrate justified confidence in security measures, processes and practices in the management of information. Whilst IA has been seen to be the growth area in recent years, maturing out of InfoSec, the ultimate goal must be to embed a full IG framework across all organisations in order to fully embrace the full breadth of information related legislation, regulation, standards, policies, procedures, technology and people issues that need to be managed, handled and protected in today's cyber dominated environment.

Course Modules

1. **Principles of IA and beyond [IA]**
2. **Standards and Best Practice Management of InfoSec [BP]**
3. **Software Assurance [SA]**
4. **Data Protection and Privacy [DP]**
5. **Records Management [RM]**
6. **Business Continuity / Disaster Recovery / Resilience [BC]**
7. **Research Methods**
8. **Dissertation**

Course Objectives

The overall objective of the group of modules provided is to develop skills and techniques in IG to ensure that when you apply these principles in your organisation you will protect the right thing in the right way, from a pragmatic standpoint with a well-Grounded Theory of understanding and will do so transparently. The IRM approach will help to ensure that you are protecting the "right thing", that is the information assets which matter most to the organisation. The technical InfoSec content will help to ensure that you are protecting it in the right way by selecting the most appropriate security control(s) which fit(s) the purpose. The IG principles will help you to do this transparently, that is, in such a way that an independent audit or assessment body can be satisfied that your measures, processes and practices comply with current regulations, legislation and standards and deliver the right level of assurance to stakeholders - citizens, customers, partners or shareholders.

Target

This MSc course in IG is carefully designed to provide a comprehensive treatment of the broad subject areas. The course should appeal to managers who would like to gain a deeper understanding of IG and the principles for good information management and handling, enabling technologies and current best practices and, at the same time, it should appeal to IT professionals who would like to gain a broad treatment of the many facets of the information at the heart of all that they will encounter. Because of the speed of changes and innovations in ICT, IG practitioners are likely to find the course (or some of its modules) useful in order to keep abreast of the latest technologies and to deploy the best IG practices.

Entry Requirements

Normally a 1st or 2nd class honours degree or relevant professional equivalent. Alternatively, a lesser qualification together with appropriate work experience may be acceptable. Recent graduates in IT or in management who would like to specialise in IG through a full-time programme. Also those already in employment who wish to keep abreast of new developments and update their skills through part-time studies or by taking specific modules in block mode. We also welcome applications from Honours graduates of other disciplines which have significant experience in the IT sector and beyond, particularly legal and ethical.

The course includes the following units:

IA Principles and beyond [IA] • IG Overview • IG Framework • IA – history – how did we get here? • Overview of relevant information-based Legislation • Data Handling Review and other Government led initiatives • IA Maturity Model (IAMM) • Culture, Ethics and Professionalism • Internal and External Audit	**Data Protection and Privacy [DP]** • Data Protection Principles • Maintaining public trust and respecting personal privacy • Information Sharing/Data Transfers – benefits and constraints • Privacy Impact Assessments • Gaining consent, Direct Marketing • Managing cookies • Data Quality management • Data breach management – and links to Security Incident Management • Data Protection in the workplace • Use of personal data in system testing Criminal Offences and the ICO's power to fine • Handling subject access requests (SARs) • Binding corporate rules • PIMS and BS10012
Standards and Best Practice Management of InfoSec [BP] • Information Risk Management (IRM), Risk Appetite and Risk Culture, Governance, Risk, and Compliance (GRC)	**Records Management [RM]** • Records Management Program (RMP) • Records and Information Management (RIM) • Standards (ISO15489) and compliance • Vital and historic records • Archives, destruction, retention schedules

• ISO 27001 and ISMS • Payment Card Industry Data Security Standard (PCI DSS) • COBIT, COSO, ITIL	• Handling records in mergers and acquisitions • RM requirements in system decommissioning • RM links with DR and backup • RM links with email management and archiving • RM links with file plan and directory structures
Software Assurance [SA] • How cyber security fits in • Threats and vulnerability analysis • Security controls (access control models and mechanisms) • Usable security • Designing security in • Firewalls and data encryption • Privacy Enhancing Technologies • Defense in depth • Cryptography • Identity Management • Human factors in security design	**Business Continuity / Disaster Recovery / Resilience [BC]** • Including InfoSec in the business continuity management process • Business continuity and risk assessment • Business continuity planning framework, BS25999 • Business Impact Analysis • Testing, maintaining and re-assessing business continuity plans • Selecting, developing and implementing disaster recovery plans • Embedding a resilience strategy • Addressing Counter terrorism in the planning
Research Methods Topics on IA and IG	**Dissertation**

10.4 Front cover of first book published 2009

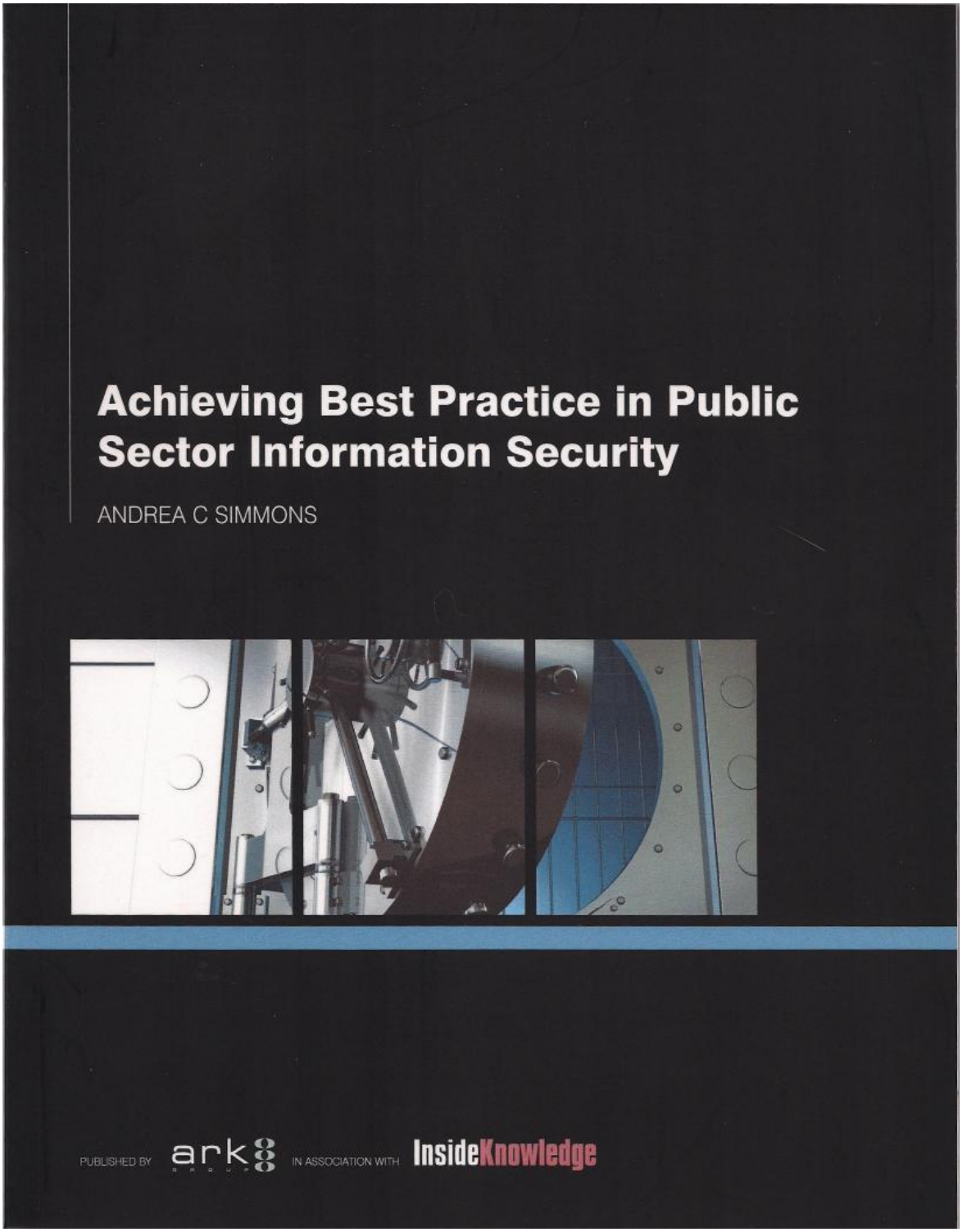


Figure 77: Simmons (2009)

10.5 Front cover of Resilience book published 2009

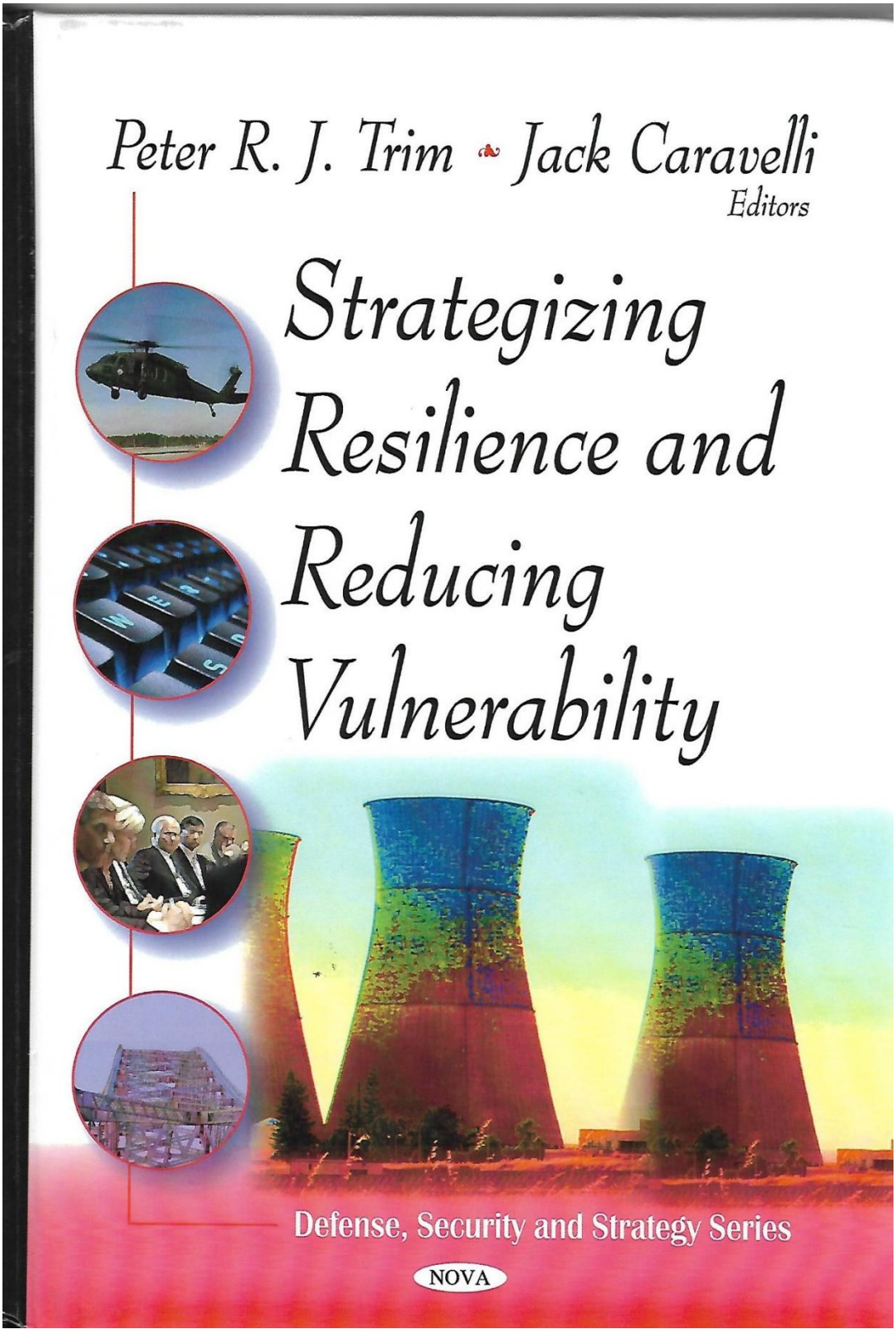


Figure 78: Trim and Caravelli (2009)

10.6 Front cover of second book published 2012

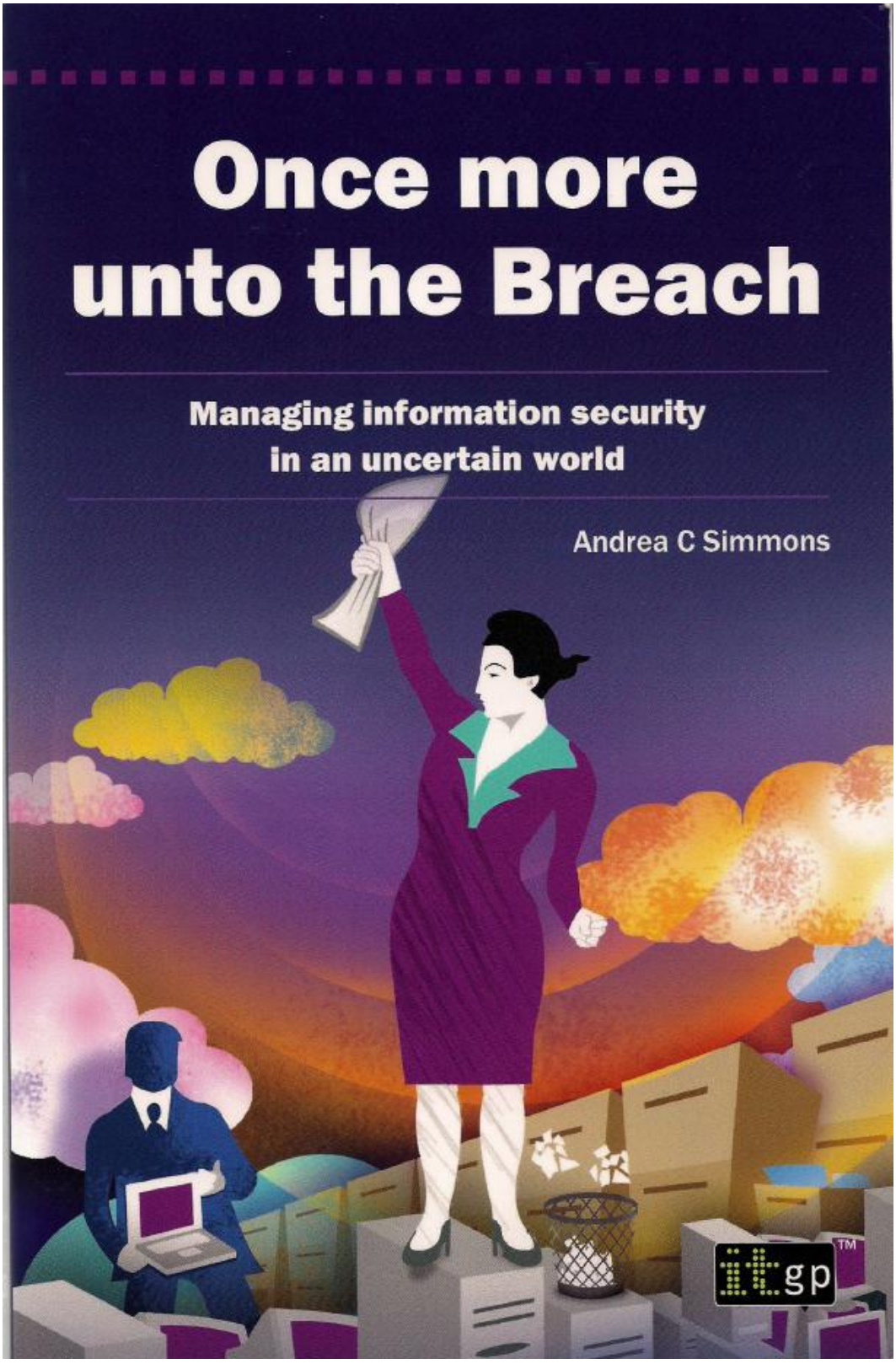


Figure 79: Simmons (2012a)

10.7 Front cover of second book reprint 2014

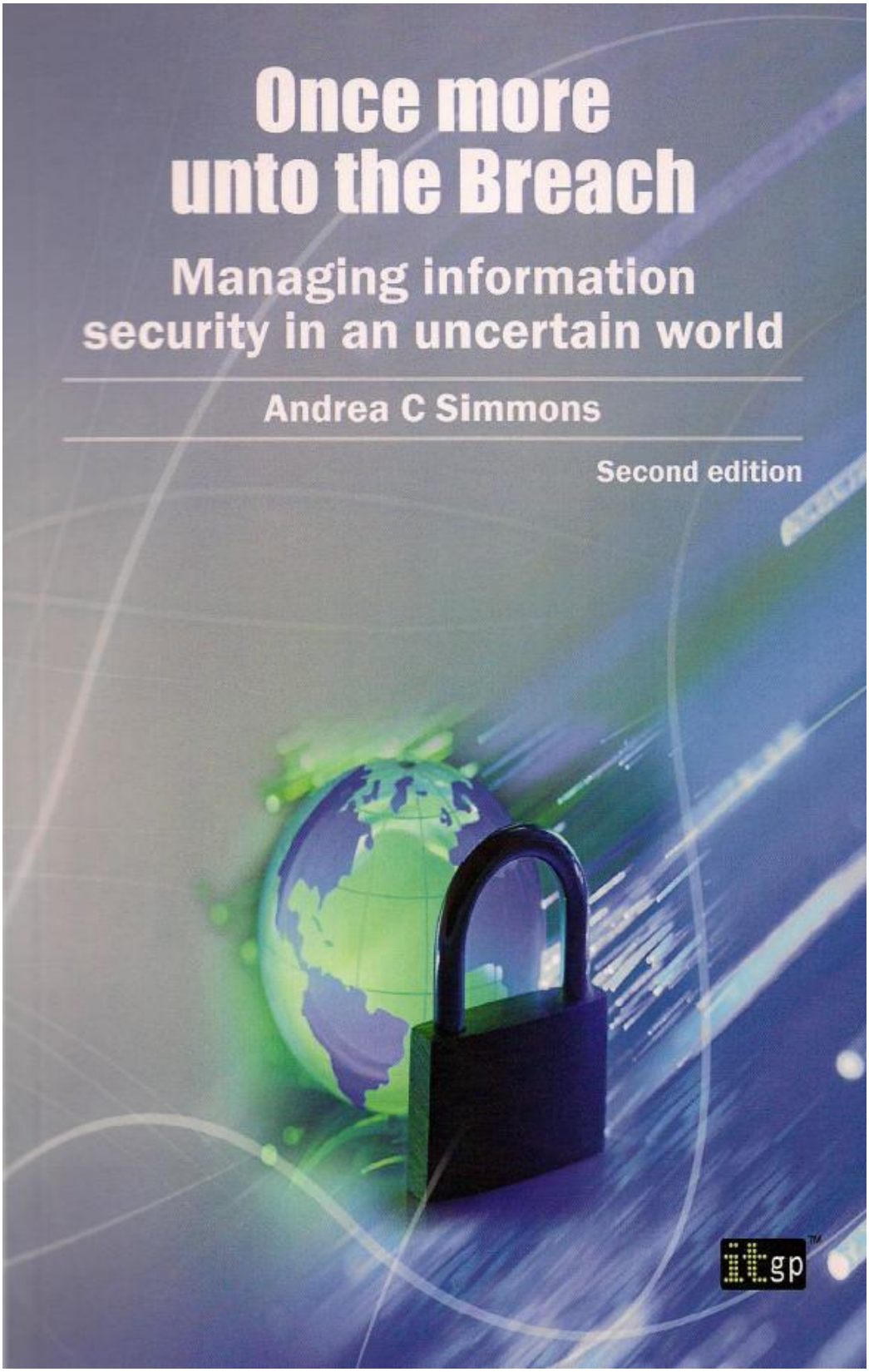
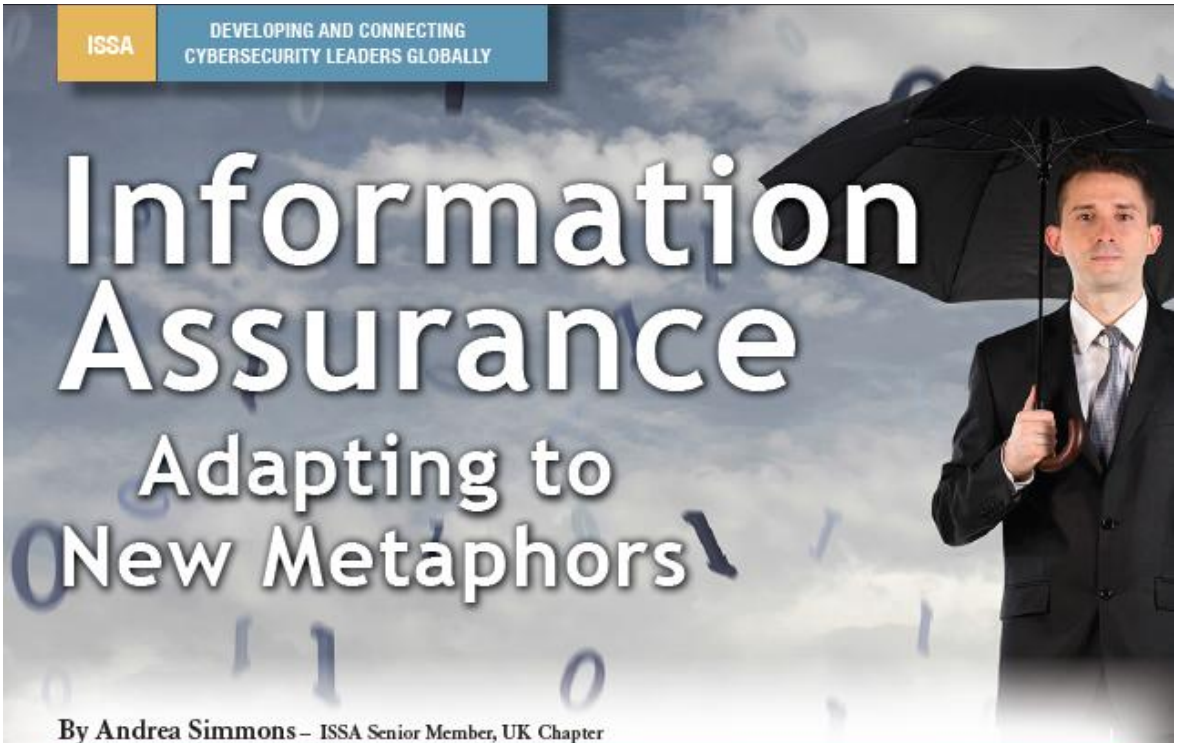


Figure 80: Simmons (2015a)

10.8 ISSA Journal Article published 2015



By Andrea Simmons – ISSA Senior Member, UK Chapter

This article discusses the route to the final conclusions of a six-year Grounded Theory with Action Research study into the usage of information assurance terminology.

I last wrote on this topic in the *ISSA Journal* in August 2012, half way through the research journey and I am now at the end of the process. This article discusses the route to the final conclusions of a six-year Grounded Theory with Action Research study into the usage of information assurance (IA) terminology. The research has been focused on philosophical and linguistic elements of terminology usage and impact, combined with a chronology of the use of IA, predominantly in the UK, tracing back the use of concepts such as information management, information security, information assurance, and information governance over a great many decades.

The aim has been to elucidate the longevity of the history available as a counterpoint to the ongoing cyber rhetoric, which the author believes is diluting the pathway to successfully providing assurance for future generations.

Given that the PhD thesis is over 90,000 words long, below will be a series of theme extracts representing the problem statement, the research questions, and the methodology utilized, followed by a number of findings, observations, and conclusions. I hope these resonate and perhaps, if you are interested, they will move you to get in touch! There is clearly much still to be done.

(Perceived) problem statement

People do not understand what the term *information assurance* (IA) actually means. This inhibits our collective ability across the public sector, private sector, third sector, and academia to adequately protect the information assets entrusted to us in order to ensure that we maintain the UK (and beyond) as a safe place in which to transact online. [Note: the UK was the focus at the start of the PhD, but following a three-and-a-half year stint in a global organization, the worldwide expansion has been taken into account.]

Methodology

The methodology was a combination of the following:

- **Constructed Grounded Theory through Participatory Action Research**—rooted in pragmatism and relativist epistemology. The research paradigm is qualitative, the methodology is inductive, and Grounded Theory lends itself to the type of study being undertaken as the process has been one of systematically looking at all the available qualitative data (through the historical review and the interview data provided) in order to generate a theory as to

why it is that IA has not been fully understood from the outset nor embedded in an holistic or successful manner.[1]

- **Historical Research**—drawing inspiration from the ethno-methodological critique of government and industry reports and similar documentary sources across all available resources (books, publications, reports), the historical method of research applies to all fields of study encompassing origins, growth, theories, crisis, etc. The author approached the research from this standpoint: "History is our collective memory. The ability to utilize history and extract useful generalizations and theories is uniquely human. Without a record of the past we are left to navigate life's course without the aid of those who have gone before us."[2]

Within the Literature Review, the intention was to illustrate the body of knowledge that exists relating to the term *information assurance*. Information security was not the focus, as this would have rendered the scale of the task all but insurmountable. The objective has been to provide a thorough review of the first decade of the 21st century (2000 to 2010)—years that were the most explosive in terms of information growth and expansion—and thus simultaneously increased information risk. However, through experience and the research journey, what has been most illuminating is the identification of so many relevant and important resources, spanning the information sciences and beyond. This has added to the body of knowledge and depth of understanding of the area, creating an extensive and wide ranging bibliography.

Three years were spent in a large UK public-sector body both observing and actively seeking to influence change within the realm of information assurance; followed by three years spent working in a US-based, global private-sector organization bringing about broad GRC changes, improving the worldwide understanding of the meaning of the *G*, the *R* and the *C* to ensure that each and everyone involved knew the importance of the constituent parts.

Throughout the process of this review into the origins of the term information assurance in the UK, the exercise has become heavily influenced by linguistics and cultural anthropology. It has been necessary to appreciate how terminology usage and interchange make a difference to an individual's ability to implement what is required, based on her own sphere of understanding.

This can be summed up as addressing the haecceity (thisness) and quiddity (whatness, essence) of IA—just what makes it what it is, including the origins of its definition, beyond that of information security. These are ancient terms grounded in ontological research and address the etymology of the subject area.[3]

Research questions

The research questions are stated to define the overall structure of the thesis and are subsequently refined during research, as follows:

1. What are the origins and original definitions of IA? The results formed the basis of the ontological question, substantiating the nature of the reality rather than the per-

1 Glaser, B.G. (1998) Doing Grounded Theory - Issues and Discussions. Sociology Press

2 Admin (2010) *Oral History: a Viable Methodology for 21st Century Educational Administration Research: National Impact, Online Education* [Last accessed on 6 June 2011] Available at: http://education-research-today.blogspot.co.uk/2009/07/oral-history-viable-methodology-for.html.

3 Aquinas, T. (1268), Summa Theologiae, London: Blackfriars, 1964–1976: I, quaest. 84, art. 7: "quidditas sive natura in materia corporali" and Norris, M. (2015) Between you and me: Confessions of a Comma Queen, page 27, W.W. Norton & Company: New York, ISBN 978-0-393-24018-4

ceptions of those who have blurred definitions over time. [Historical Research]

2. Are these definitions well enough understood and appreciated at the appropriate levels to be able to implement the requirements, both now and as they develop over time? [Survey & Interviews]
3. How important is reading available literature as part of the learning process to support IA professionals in doing their job effectively? [Survey & Interviews]
4. How does the ability to do so, or not, support the advancement of the Information Society? [Participatory Action Research (PAR)/Case Study]
5. What impact has change of political leadership had on the route map of IA across the UK public sector—in the context of policy making and professional practice? [Mixed Research Methods]
6. What other barriers to successful implementation of IA can be identified through historical review and research of available materials and observation of human interactions? [Mixed Research Methods]
7. How do the answers from the previous questions support the development of the IA profession? [Mixed Research Methods]
8. What should the ethics requirements be for IA professionals? [Mixed Research Methods]

The aim was to identify consistency of understanding in order to ensure, as an industry, we have a firm footing of understanding as we seek to continue to professionalize. In short, we don't!

Questionnaires were sent to a number of key groups and audiences; some interviews were also conducted; the findings have been analyzed and the results have been used to formulate the theory.

Setting the scene

It's all about the importance of language and terminology usage, given that IA can mean information assurance or internal audit; IRM can mean information and records management or information risk management. People get confused. And people do not know the basic principles behind all this—the security principles of CIA (see below)—and the fact that this does not mean Central Intelligence Agency. It impacts the "cyber skills crisis"—given that in reality there is more of a "cyber understanding crisis." Just relabeling everything as *cybersecurity* didn't make it different. It didn't make our operational security needs different. All the recent, high-profile breaches are showing that the root causes are a combination of human error(s) and a lack of operational security hygiene.[4] Cybersecurity, in the grand scheme of things, will be a short-term bandwagon. Long-term strategic risks for organizations require knowledge of the criticality of information.

You only have to Google "skills crisis" and a plethora of results will appear.[5] "My" Google is well trained after six years of PhD research into all aspects of the origins of the usage of the term information assurance! If I type information, all my devices assume that the next word is assurance! However, if my photography-loving husband typed skills crisis into his Google search bar, a different set of responses would arise. This is entirely in keeping with the findings that suggest we have the same linguistic terms available but can end up attributing different meanings, priorities, risks, and issues to them.

This was more starkly brought home in doing some background catching up on the keynote videos from Infosec 2015,[6] where a renowned colleague made a direct challenge to a panel on the subject of "actionable intelligence." It is yet another of those "spin" type terms that have seeped into the core of our organizations as a result of clever marketing endeavors. If you are from a military background then intelligence has a specific meaning, connotation, and implication. If you are of an academic persuasion, your context of understanding for the use of the term will be different again. I use these examples quite deliberately to illustrate what so moved me to devote quite literally every spare waking hour of the last six years, part-time, on top of a full-time information security role, to diving deeper and deeper into identifying the level of actual understanding available with regard to the term information assurance and related terminology, on the premise that it is having an impact on the lack of successful adoption of the delivery of IA.

There appeared to be a gap in the absorption ability worth investigating in order to solve what turns out to be a "wicked" problem.[7] IA is not a project. There is a body of literature both in professional practice and in the academic world. The research has sought to undertake analysis (breaking it down), reviewing the constituent parts, influences, changes over time, and then undertaking synthesis—putting it back together and evaluating whether IA remains fit for purpose for some time to come.

We are living in the age of Twitter where a news story, however brief on fact or content, will be around the world in minutes. Studies are showing that attention spans are dropping still further.[8] People will neither attend nor sit through training sessions for more than fifteen minutes now. You cannot learn anything meaningful in detail in that time. (It still takes seven years to become a doctor for a reason after all). Everything is being "dumbed down"—invariably to remove technical detail, though usually as a claim to seek clarity of understanding, which is a misnomer. Shrinking minds is

4 Read this – excellent write up issues WE all know about... http://gizmodo.com/9-facts-about-computer-security-that-experts-wish-you-k-1686817774.

5 Check this out for a more general view: http://docs.media.bitpipe.com/io_10x/io_102267/item_465972/Were_just_not_doing_enough.pdf.

6 View InfoSec 2015 Keynote sessions online here - http://www.infosecurityeurope.com/media-centre/video-channel/2015-keynote-videos/.

7 Rittel, H. W., & Webber, M. M. (1973). Dilemmas in a general theory of planning in Policy Sciences, 4(2), 155-169, [Last accessed 6 August 2015]. Available at: http://www.cc.gatech.edu/~ellendo/rittel/rittel-dilemma.pdf.

8 http://www.huffingtonpost.com/2013/10/24/attention-span-book_n_4151059.html.

leading to shrinking value, and yet we live in an information-abundant era.

There is Risk Myopia—an ability to not see the big picture nor believe it when it is explained to you. In 2003, I was involved in a UK government-sponsored study entitled Cyber Trust and Crime Prevention, engaging with industry, academia, and government colleagues alike, to identify the likely future challenges and seek to address these through policy changes, education, and awareness. There were detailed reports produced at the time and various follow-up opportunities. However, as recently as June 2015 a UK Police Commissioner refused to believe me that we were talking about the "cyber" thing as far back as 12 years previously. Ignoring the blatant element of sexism involved in the exchange (a separate ethical issue raised in previous *ISSA Journals*, I am pleased to note)—this blindness is very much at the heart of my study. There are people in power who lack sufficient grounding in the history of how we have got to where we are and what the broader issues might be.

Those in charge of policy making and in conducting certain activities do not know enough about the actual subject area in which they are charged with making important decisions and thus they cannot make effective risk judgments nor lead to sensible outcomes, a sentiment captured by Funston, below:

> "If people don't know that they are incompetent in an area in which they are trying to solve a problem, their solution is likely to be suboptimal".[9]

9 Funston, F. and Wagner, S. (2010) *Surviving and Thriving in Uncertainty: Creating the Risk Intelligent Enterprise*, John Wiley & Sons, ISBN-13: 978-0470247884.

This is of some significant concern, given the evidence of management hubris coming to light through the post incident reviews and aftermath of data breaches. Clearly there is also risk (analysis) paralysis—evidence of incomplete risk understanding, incomplete risk documentation; evidence of inaction—all of which amount to shouting about risk in a vacuum.[10]

Context and methodology

This study, begun in 2009, includes an extensive historical journey of the origins of the usage of the term *information assurance*, how it is intrinsically linked with the term *information security* (infosec), in an attempt to explore the reasons for the lack of successful adherence to existing principles. Taking as a guiding driver two key objectives from the 2011 UK Cyber Security Strategy[11]—**Objective 1**: tackling cybercrime and making the UK one of the most secure places in the world to do business; **Objective 4**: building the cross-cutting knowledge, skills, and capability to underpin all cybersecurity objectives—the author has sought to research these objectives with a view to understanding how they could be achieved, if the principles behind the requirements are not fully understood. The outcomes have been an opportunity to revisit the available ontology for information assurance and provide a long view into the future.

The thesis has specifically targeted the complexity of terminology usage and the challenges presented by lack of understanding of the fundamental principles behind the terminology used as being a central cause of the skills crises. The premise is that issues related to professionalism in the industry, the skills crisis, and achieving the culture change required in order to embed information assurance as a core functional area of any organization are all related to a lack of understanding of the terminology being used and the contextual meaning of the words. If ignorance continues to prevail, information protection will not succeed.

Following an examination of the aforementioned history and constraints, combined with a comparative case study between public- and private-sector experiences, the investigation considers existing ontology, adding to the body of knowledge by providing the next iterative step. A grounded theory has been used to design a new combined ontology, branded as i3GRC™ (integrated and informed information governance, risk, and compliance), which advocates holistic thinking across the operational landscape in order to best protect the information at the heart of all organizations. Conscience of the length of this article already, a detailed description will have to wait for a future edition when governance is the focus.

Given the purpose of ISSA and its worldwide membership, the following should all be known. This is a challenge we face in the industry. We all attend meetings, read journals, blogs,

10 Hillson, D. (2014) *The Risk Doctor's Cures for Common Risk Ailments*, pages 127 and 145, Virginia: Management Concepts Press, ISBN: 978-1-56726-459-3.

11 UK Cabinet Office (2011e) The UK Cyber Security Strategy Protecting and promoting the UK in a digital world, November 2011, Ref: 407494/1111, Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf [Last accessed 3 May 2015].

and articles about our own space, and talk to each other about a subject we all know or write about ourselves. Yet, still the changes required are insufficient; the level of embedded practice is not taking hold; the "build security in" mantra has not been adopted—as can be seen by the ongoing data breaches continually being reported in the news. Invariably, it turns out that the original chink in the armor was something basic, a fundamental of security management tenet that should have been in place, that should have been addressed. More worryingly, there have been security professionals involved at some point in the journey of all the organizations experiencing breaches. So what's going wrong? Why are they not being listened to? These are the questions that keep me awake at night! This is what started my journey six years ago, which shows how little progress there has been.

Historical context

As in life, most things have an evolutionary cycle, a maturity path. The information space is no different. The value of information and the need to adequately protect it have been important societal tenets for centuries. We are living in an interconnected Information Age where there has never been greater access to information nor adoption of technology. The Information Society has progressed apace, significantly enhanced as a result of the speed of technological developments and the reach of the Internet to parts of the world previously unconnected. The speed of development in many industries, in and of itself, leads to skills crises.

Legislative, regulatory, industry standards and political changes can be shown to have had a significant impact on the understanding of requirements for information protection within the information society. Industry experts have been articulating the subject of information assurance, the reasons and need for it for several decades and yet progress to successful adoption still lacks corresponding speed in alignment with the pace of the Information Society, as evidenced by the increased volume of data lost or stolen and the number of systems breached.

If we start as below for a high level, it will help us keep our bearings:

1. Physical Security
2. Communications Security (COMSEC) ['40s]
3. Operational Security (OPSEC) ['50s]
4. Automated Data Processing Security ['60s]
5. Computer Security (COMPUSEC) ['90s]
6. IT Security (ITSEC) ['90s]
7. Information Systems Security (INFOSEC) ['90s] - merged COMSEC and COMPUSEC following rapid change in technology; combined in a new paradigm to become INFOSEC, internationally recognized in Common Criteria

The Curmudgeon – Really Useful Solutions

"He who can, does. He who cannot, teaches." George Bernard Shaw

THERE'S AN INTERESTING FOLLOW-ON: Those who cannot teach, teach teachers. Those who cannot teach teachers, administrate.

Full disclosure: I've done, taught, then taught others to pass along knowledge, and now I'm writing about all the rest. I guess, if I were applying to HR, I'd be "overqualified." Either that, or I've gone well down the slippery slope. Oh, My Goodness! The next thing, I'll consider becoming a lawyer or a politician! Somebody shoot me now!! (Head shot, please. Let's finish the job.)

This month's theme: Academia and Research. Both are overloaded terms (in the software sense). I'll settle on *Academia* as formally accredited schools offering degrees or for-profit organizations offering technical training.

Academia is great for theory but lacks application for the information security industry. It is a "band wagon" situation. Long after the need is identified, they finally begin offering courses, papers, and explanations of how it "ought to be," rather than dealing with things that are already in the wild.

Research suggests a few conditions: research into existing products and their (lack of) security features; research into what works to defend systems against unauthorized activity; and "research" into theoretical approaches that are de facto limited. While one might publish volumes for the latter, it is useless. The second is far more interesting but always fights a holding action. The former gathers the limelight, but fails to add substance since all it says is "Look! I can break this." In general, they offer no fix, but only exhortations to "fix it."

A few years back there was a *Journal* article about how small businesses could deal with "information security" on a practical basis, an inexpensive basis. It received a couple of comments amounting to "At last! Something we can USE." In the next issue, the idea was lost to sight in the swell of academic and research articles. That somewhat calls into question what the community is trying to accomplish.

If I were in a corporation and sought someone for my IT shop, and better yet, my information security, assurance, or whatever staff, I'd want to see a few battle scars on those resumes. I don't care what you published. What did you actually do? What crises did you handle, and how? Was it you, or someone with a really good idea you took credit for? I have all of the latter I can stand.

Now to make peace: If you are in academia and have the Next Great Idea, take it to the next stage: how might it be implemented In The Real World (ITRW)? If you're a "security researcher," and you've figured out how to break something, how can they fix it ITRW? If you teach this stuff, but do not actually teach people how to fix things, update your presentations: "If you run into this, here are some things to consider...." And if you're just teaching the teachers, you'd best look out. You'd better give them actual solutions to pass on or get ready to get hit in the backside by the doorknob.

Really useful solutions, made available to your audience. What can you do today to put that into practice?

Your local, grumpy, tie-wearing, un-impressed, and suspicious Curmudgeon

8. Information Assurance ['00s] (but cyber threats being investigated in the background)
9. Cyber in the media….. ['10s]
10. Internet of Things/Information Society ['10s]

I have no doubt many of you would articulate that differently, add a few more in, shuffle them about a bit—but you get the idea! One survey respondent articulated it thusly:

> Security > IT Security > Information Security > Information Assurance > GRC : It's an evolution. In this dynamic world, we learn, unlearn, and relearn. [Respondent X, APJ]

In a similar vein, another IA scholar identified and articulated "Security epochs"[12]:

1. Revolutionary War to the mid-1820s, mid-1830s to the 20th century ending with WW1
2. WW1 and Soviet Union emerging
3. 1920 to 1946 global recession, rise of international communism as Europe collapsed—leading to American democracy crisis
4. Cold War
5. Information Age—technological developments, chemical and biological weapons, etc.
6. Cybersecurity through to the Internet of Things

If you take number 3 above—it is clear that as humans our ability to repeat patterns of behavior indicates an inability to learn lessons from history, in spite of all the perception of progress.

This has recently been the focus of a McKinsey report,[13] identifying the following:

- Pre-2007 — Cybersecurity not a priority*
- 2007-2013 — Cybersecurity as a control function
- 2014-2020 — Digital resilience**

* Not entirely true, given the available material and those for whom it has been a priority for a long time. ** This corroborates my findings and conclusions that *cybersecurity* is "not long for this world" in terms of focus and will be replaced—but ultimately all of this still represents a need to ensure good information security controls are in place and that an information assurance framework is in operation to provide oversight and governance.

Definitions, models, and frameworks

I write this knowing that our venerable colleague Donn Parker until recently produced his regular *Donn's Corner* column for the *ISSA Journal*, one which I urge you all to re-review, in particular the axioms! Take as the starting point Donn's column in the July 2015 *ISSA Journal* entitled "Information Security Defined."[14] As an information security professional, I can wholeheartedly agree with the "fundamental model" provided. However, as an academic pedant, I would have to counter that in actual fact what was articulated was a definition of information assurance.

During the research, one respondent observed others commenting that "….the difference between information security and information assurance is that between the private and public sectors." The more I think on it, the more interesting the comment becomes. [Respondent Y, UK, 12 November 2010]

The author believes this is both interesting and challenging, given it is erroneous from a number of angles. Let's go back a step or two and confirm some available definitions.

12 Hamre, J. (1998). Information Assurance and the New Security Epoch. *USIA Electronic Journal*, November 1998.

13 Kaplan et al (2015) *Beyond Cybersecurity:Protecting Your Digital Business*, McKinsey, Wiley, May 2015, ISBN: 978-1-119-02684-6.

14 Parker, D. (2015) "Information Security Defined," in Donn's Corner, page 23, *ISSA Journal*, July 2015.

Information security can be defined as the "preservation of confidentiality, integrity, and availability of information" and focuses on the controls required to protect the information at the heart of an organization. This is invariably represented as the CIA triad, or triangle (figure 1).

Figure 1 – The information security triad: confidentiality, integrity, availability

In a climate where regulation around information security and regular "data leakage" stories in the media battle against budget constraints and reduction, it is crucial for organizations to ensure that any spend is targeted and business-focused to maximize return on investment. Clearly this is easier said than done and involves a depth and breadth of control (safeguard) implementation following risk assessment, etc.

The confusion sets in when multiple interpretations are allowed. The representation in figure 2 requires explanation [found on an extremely helpful blog in 2011 by Salvador "GRECS" Grec[15]]; while on first sight it makes perfect sense and is acceptable, with knowledge brings the ability to question and seek greater clarity.

Figure 2 – Information security a subset of information assurance

The right hand bubble actually represents more of a description of IT security, while the outer ring labeled *Information Assurance* more accurately represents *Information Security* in the ISMS, ISO27001 sense. (Enter into the domain of the definition pedant—although I know I am not alone!)

Information assurance is defined more in line with Donn Parker's articulation—adding authentication and non-repudiation onto the CIA. The basic meaning of information assurance is captured by the definition from the US National Information Systems Security Glossary,[16] which is as follows:

> **Information Assurance (IA)**: Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

IA is broader than infosec. There are degrees of assurance. The term itself is born out of the military domain and had specific connotations at the time. The pictorial representation in figure 3, found in another thesis,[17] shows this clearly, given the placement of IA (on the left hand side).

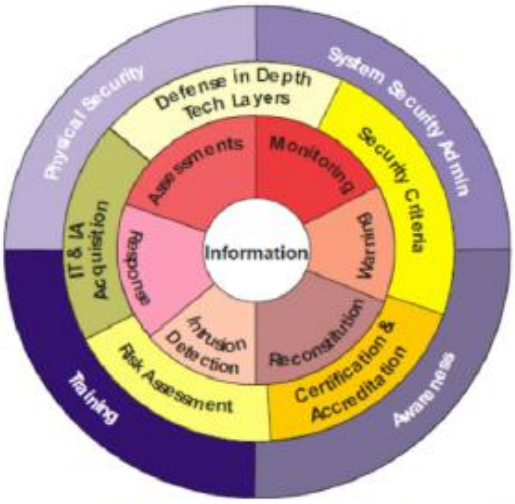


Figure 3– Representing defense-in-depth layered defense model

"IA" as labeled in figure 3 is actually referring to "security assurance"—the ability to evidence the trustworthiness of systems and their design, when the daily lexicon involves reference to Common Criteria[18] and "the Orange Book" with Evaluation Assurance Levels ratings, etc. This a subset of information assurance in line with quality assurance practices. Unfortunately, this appears to be an aspect that has not been followed through to the wider industry, given the ongoing malpractice evident in the breaches experienced—for both budget and time-to-market reasons.

In the most simplistic terms, the expansion between infosec and IA can best be represented by figure 4—with the green representing infosec and the blue additions representing IA, once you put it all together. We have the infosec triad showing the CIA elements above and the IA five pillars—CIA plus authentication and non-repudiation.

15 https://www.novainfosec.com/2011/08/30/information-assurance-versus-information-security/.

16 National Information Systems Security (INFOSEC) Glossary, NSTISSI No.4009, Aug. 1997

17 Nanton, T.I. (2004) Achieving Information Assurance, USAWC Strategy Research Project. US Army War College, Pennsylvania, [Last accessed 10 August 2015] Available at: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA424379.

18 Common Criteria for Information Technology Security Evaluation, August 1999, [Last accessed 1 March 2015], available at: http://www.commoncriteriaportal.org/.

Figure 4 – The IA five pillars

These pillars are supported by five common aims[19]:

1. Prevention
2. Detection
3. Containment
4. Deterrence
5. Recovery

The most recent description of the alignment between assurance and security can be found in an independent review of the security measures surrounding the UK Census 2011, which echoes the reference to Common Criteria above:

> The term "assurance" has a specific meaning within the security environment. Assurance is gained through activities confirming that the security measures that have been set in place are both effective and appropriate. It is not sufficient simply to set in place an assembly of technical and procedural controls; they must work, they must be seen to work, and they must be aligned to the underlying security problem.... Assurance confirms that the security measures that have been put in place are aligned to the problems that they are intended to address, and that they can be relied upon to operate as expected.[20]

There are existing industry standards (e.g., ISO27001, PCI), legislation and regulation (e.g., HIPAA, FISMA, DPA, GDPR), and available body-of-knowledge repositories (e.g., ISACA, ISSA, BCS, IISP) that rely on specific sets of wording. They use a body of knowledge for a reason—as they are a compilation of the available knowledge, wisdom, and experience of many who have gone before, combining the efforts and understanding of people, process, product, and proof (of successful implementation). Therefore, seeking to redefine existing concepts is not helpful. Organic growth and maturity is one thing, but redefinition is inappropriate.

High-level overview of findings

All organizations require clear security policy requirements supported by executive management. In order to effectively implement and adhere to these requirements, what has been learned is that there is a real need for a depth of understanding that is not present due to a combination of a lack of experience and a lack of relevant education. Too many security "professionals" are self-taught. This has led to a serious dearth of knowledge. In order to improve the situation, clear leadership is required, supported by clear and consistent communication in order to aid understanding. This requires accountability and responsibility across the whole organization, particularly including human resources/personnel in order to ensure that an enforcement structure is in place; otherwise the strength of the requirements is rendered meaningless. Roles and responsibilities need to be defined in order to effectively apply and ensure consequences for inaction or non compliance exist.

The interpretation of the results—people involved in information security do not understand the language of it—is what has led to the formation of the grounded theory that leads to the need for the improvement framework (i3GRC). It has been important for the author to produce a theory that fits with the real world and is grounded in the empirical data.[21] In so doing, an appreciation of design science research has also been realized.

When we put the history back together and work out the basics — and obviously you can assume that for the sake of the length of this article, I am leaving large chunks out!—there is a point at which there are some other fundamentals you need to know about. One of these is the OSI Model[22]—represented in figure 5.

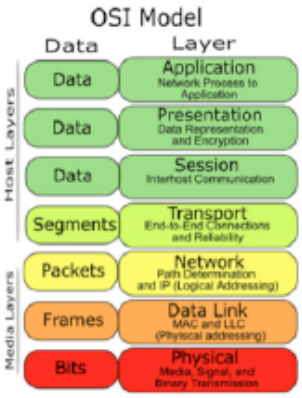


Figure 5: The OSI model

In our interconnected information society, we now have to consider two other clear layers above the seventh, application:

- **Layer 8 – People**—human factor/wetware, the carbon layer. We cannot control stupidity.
- **Layer 9 – Politics**—internal to the organization in which you find yourself working, as well as external, both within country and beyond, given the level of outsourcing we are

19 Schou, C. and Shoemaker, D. (2007) *Information Assurance for the Enterprise: A Roadmap to Information Security*, page 62, New York: McGraw-Hill Irwin, ISBN 10: 0-07-225524-2 / ISBN 13: 978-0-07-225524-2 / ISBN-13: 978-0-07-225524-9

20 Dowdall, J., Mattinson, H. and Fagan, P. (2011) 2011 Census Security: Report of the Independent Review Team, ONS, January 2011, [Last accessed 25 May 2015]. Available at: http://www.nisra.gov.uk/archive/census/2011/2011_Census_IIAR.pdf.

21 Gregory, R. W. (2011) Design Science Research and the Grounded Theory Method: Characteristics, Differences and Complementary Uses, In Theory-Guided Modelling and Empiricism in Information Systems Research, Berlin: Springer ISBN 978-3-7908-2780-4

22 http://www.comptechdoc.org/independent/networking/protocol/protlayers.html.

all balancing and the cross-geographic boundary working that involves multi-jurisdictions.

There are so many possible examples to be shared regarding the above, many of which are regularly covered by the excellent contributions in this journal, month in and month out. As a security professional, living in the information age, the job writes itself on a regular basis (Carphone Warehouse is the latest casualty hot off the press at the time of writing[23])! The Web has provided undeniable connectivity and information exchange opportunities, much of which are to be welcomed. But regularly one wonders as to the sanity of decisions made when, for instance, there are data centers and military installations available on the Web, under the guise of public relations, signposting their buildings and facility locations. Just because you can, doesn't mean you should—as the meme goes.

This way lies information governance

The information security profession expanded to adopt the use of the information assurance term. However, current populist usage of the *cybersecurity* term is actually creating a contraction, in both words and deed. It is not as all encompassing, given that it only reflects the medium, not the overall business aims. Research has led into the wider world of information governance in order to best address the breadth of the scope of information protection required in the information society of the 21st century. There is a point at which information assurance (IA) and information governance (IG) must coalesce in order to be a more effective and holistic whole.

The Information Governance Initiative[24] defines information governance thusly:" the activities and technologies that organizations employ to maximize the value of their information while minimizing associated risks and costs."

The author prefers the more broad view of information governance as a holistic approach to managing corporate information by implementing processes, roles, controls, and metrics that treat information as a valuable business asset.

Information governance—as per Gartner—is the specification of decision rights and an accountability framework to encourage desirable behavior in the valuation, creation, storage, use, archiving, and deletion of information. It includes the processes, roles, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.[25]

This is quite an IRM-centric view where, in this case, *IRM* stands for information and records management. A further refinement reaches this result: "Information governance is the setting of objectives to achieve valuable outcomes by people using information assets in a life-cycle process that considers the impact of both risk and time." [26]

In list form, seven words cover the whole domain, all of which are aspects we all, as information security professionals, address on a daily basis:

1. Objectives
2. Outcomes
3. People
4. Assets
5. Process
6. Risk
7. Time

Information governance sits within the information sciences. However, if we look wider, we find that the information management (IM) profession is, in real terms, divorced from the information security profession in outcome and output terms, the clear link being...information! Given the pace of pressure for the general populace to engage with the information society and adopt the ways of the interconnected world, all the information-related professions have a pressing need to gather together and meaningfully address the challenges highlighted. IT, IS, IA, IG—are all on a continuum—with IM running through them. Depending on your viewpoint, however, you could write that differently. For example, IM, IT, IA, IG are all on a continuum, with IS running through the horizontal as the *I* needs to be secured in all its forms and throughout the life cycle.

In order to address *Big Data*, there is a need for the use of data scientists in the information security space in order to improve management reporting within the information assurance landscape, to better interpret the volume of spreadsheet overload and log monitoring data dumps. It is hoped that this will bring the worlds of IG and IA closer to an ultimate amalgamation and consolidation of functions and roles in a greater understanding of the information oil at the core.

While IG is not synonymous with corporate governance, it can be considered to be more akin to "GRC for information," and the metrics element is vital, given the need to explain to management and leadership the return on investment. As per the wheel at figure 6,[27] the coalescence point is driven home by the spread of coverage identified. Not forgetting that to the rest of the business, IA stands for *internal audit*. This article would have taken more prefacing were it written for ISACA, for example! Internal audit provides an opinion on the veracity of the management assurance. This will include information assurance—assurance that you have done what you said you would do to achieve a risk posture that suits the needs of the organization. Governance provides board-level reassurance.

23 http://www.theguardian.com/technology/2015/aug/10/carphone-warehouse-uk-data-watchdog-investigating-customer-hack.

24 http://igiinitiative.com/.

25 https://lenand.wordpress.com/tag/gartner/.

26 Ibid.

27 http://ethicalboardroom.com/wp-content/uploads/2014/12/Baron_figure1.jpg.

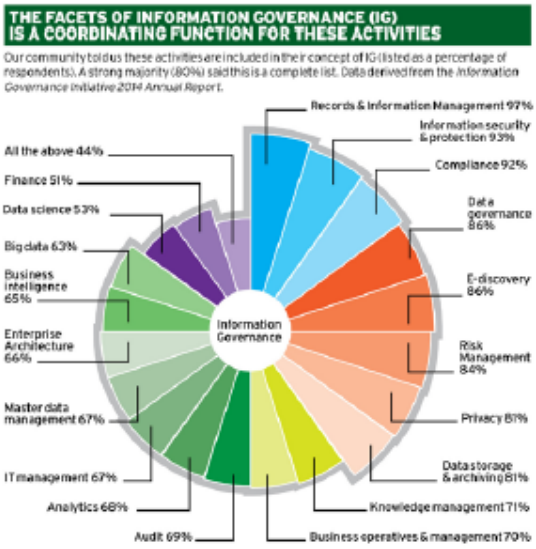


Figure 6 – The facets of information governance

Conclusions

Enough of the right people do not know the ontology of Information Security (Infosec). Enough of the right people do not know the ontology of Information Assurance (IA).

Therefore, enough of the right people will not know nor be able to see the relationships between infosec, information security, and information governance. Much work has already been done in this area and plenty of resources exist. A reference link to some of the outputs are available.[28] While the CIO role goes through ongoing transformation and the CISO role continues to a poisoned chalice for many (a subject for another article in itself!), the near-term future will see more CIGO roles—Chief Information Governance Officers—for those who can see the bigger picture and can holistically bring all the strands together.

Knowledge, leadership, and communication are at the core of our success in the future. I know that we all know this. However, multiple attempts to engage with boards and directors do not appear to have created the kind of enlightenment required to provide embedded security. There is a level of middle management still blocking necessary actions being taken.

> *The single biggest problem in communication is the illusion that it has taken place.* (George Bernard Shaw)

The conclusion of this research is that we are at a crossroads where information assurance either needs to combine with another complex system—the author would suggest this to be information governance—or it will be lost forever to the realm of "cyber" and, as a result, a dilution of intent and ongoing breaches and bad security implementations will continue to be the experience for the remainder of the 21st century. As a result of the language used, there is a contingent impact on the culture of an organization in terms of its willingness to adopt the messages provided and embed the best practice advice.

Information assurance, in and of itself, is not a core discipline—in business nor in academia—and can thus never be a profession nor academically accepted. That's a cold hard fact. Something has to change. We need an IA governing body, one that will inform of updates. The BSI hosts the significant effort of updating the ISO27000 family of related standards.[29] If IA is to survive, there needs to be something similar.

The protection of information resources through the activity of information assurance is a defining challenge as the landscape of information warfare continues to mutate in the onslaught of cyber attacks—made only worse by the self-inflicted wounds of many organizations who leave themselves open to attack through bad practices.

These challenges require that we turn to the expertise of information professionals in the broadest sense to protect systems vital to all of us. The research survey questions led to wider societal- and industry-related questions with pithy conclusions:

- What is required? IA professionalism
- Who is it for? IA professionals
- What's the benefit? Better designed and protected systems of systems from the outset; less breaches; less loss of income; less impact to industry, individuals, and society as a whole.

Key learning

It has all been said! (Though maybe that is an aspect of doing a PhD later in your career and having a longer vista over which to review many threads!) As a fine example of this reality, while you may think Donald Rumsfeld coined the phraseology around unknown unknowns, Confucius allegedly said it first: "To know that we know what we know, and that we do not know what we do not know, that is true knowledge."

References

An extensive bibliography is available separately; please contact author.

About the Author

Andrea C. Simmons, FBCS CITP, CISM, CISSP, M.Inst.ISP, MA, has more than 17 years direct information security, assurance, and governance experience. Her most recent role as CISO for HP Enterprise Security was one of worldwide influence, addressing security policy and risk governance, seeking to support and evidence the delivery of organizational assurance across a wide portfolio of clients and services. She may be reached at andrea.simmons@wlv.ac.uk.

28 See for example: http://www.eurim.org.uk/activities/ig/ig.php.

29 http://www.bsigroup.com/en-GB/iso-27001-information-security/.

Figure 81: Simmons (2015b)

10.9 ISSA Journal Article published 2012

ISSA DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Understanding Control Standards within the Context of Standards, Compliance and Governance

By Andrea C. Simmons – ISSA Senior Member, UK Chapter

This article discusses control standards in the context of how we apply these internally across our organizations, as opposed to industry standards that apply more broadly. It seeks to step through the terms and refresh the thinking on how we should be aligning them in the context of compliance and governance.

Abstract

This article discusses control standards in the context of how we apply these internally across our organizations, as opposed to industry standards that apply more broadly. This article seeks to step through the terms and refresh the thinking on how we should be aligning them in the context of compliance and governance. These are challenges faced by many security officers on a daily basis, in terms of the implementation of the control standards set before them, as well as a challenge for the audit teams (both internal and external) who have a need to assess compliance against them. Please note, the views expressed are the author's own and should not be taken as indicative of an agreed corporate view. These observations are based on daily interactions with board members, executives, line of business, internal auditors, risk managers, security officers, consultants, and external auditors.[1]

Setting the scene

Both the British Standards Institute (BSI)[2] and the European Technical Standards Institute (ETSI)[3] define standards as, respectively, an agreed, repeatable way of doing something or a set of rules for achieving quality. I am using the term *standards* in the sense of security standards required to provide consistent and coherent corporate messages regarding the implementation of security policy requirements and security architecture.[4] These are often referred to as control standards (or controls), to identify those elements that an organization may need to adhere to in order to maintain a particular security posture. The aim is to implement a control system. The security industry has taken this term – *control standards* – from the financial and accounting industries. Controls exist in Quality circles and in Engineering, too. Engineering controls are precautionary measures that isolate or remove hazards from the workplace and include safer medical devices, self-capping syringe needles, ventilation systems such as a fume hood, sound-dampening materials to reduce noise levels, safety interlocks, and radiation shielding.

Standards, compliance, and governance

With this kind of context, it is easier to see why our internal security standards are referred to as controls, as they are intended to reduce many different forms of risk – strategic, compliance, financial, operational, political, environmental, etc. – by providing us with a control system so that we are operating within a framework of shared references.

By now, most organizations have many internal controls in place as a result of a need to comply with a raft of legislation-, regulation-, and industry-specific standards. For example, we have the Payment Card Industry, Data Security Standard (PCI DSS) requirements which have been translated into security controls for addressing those requirements. We also have the option of selecting, through risk assessment, any of the avail-

1 I am researching the origins of the usage of the term Information Assurance in the UK and whether or not its ongoing usage is proving to be effective – as opposed to, say, Information Security, or Information Governance.

2 www.bsigroup.com.

3 www.etsi.org, http://www.etsi.org/WebSite/Standards/WhatIsAStandard.aspx.

4 http://www-935.ibm.com/services/hk/en/it-services/security-standards-definition.html.

able 132 ISO 27001 controls (also referred to as safeguards and countermeasures). We have ITIL and COBIT. We have NIST guidance, which comes in many forms – and again can be recreated internally into appropriate control standards to be adhered to. We have health care regulation and legislation requirements. We have data protection and privacy requirements, records and information management requirements, security architecture, design and build requirements – all requiring standards of adherence. And many of us now have International Standards for Assurance Engagements (ISAE) No. 3402 and Service Organization Control (SOC) reporting to address. There are many others which will no doubt be referenced in other articles.

Compliance

Then we have compliance, which is a function carried out by a team whose role should be to ensure that appropriate measures are in place to enforce and constantly check and update the policies that support the confidentiality, integrity, and availability – i.e., Information Security – requirements as set out by management. That *update* piece is an important one to note: policies, procedures, standards, and guidelines are not written in a vacuum, nor set in stone. They must be fluid and flexible enough to be changed as suits the organization and its requirements, as well as its risk posture.

To be compliant, means to be in conformance with stated requirements (including controls and procedures where mandated to do so). At an organizational level, it is achieved through management processes which identify the applicable requirements (defined, for example, in laws, regulations, contracts, strategies, and policies), assessing the state of compliance, assessing the risks and potential costs of non-compliance against the projected expenses to achieve compliance, and thence prioritizing, funding, and initiating any corrective actions deemed necessary. It should be seen as being a very proactive and engaging activity, rather than a static, inward-facing role. If our users are consistently not doing a particular security requirement, not following a control, not adhering to policy, it may very well be that what we have written is simply not intelligible to them and they are never going to appear to be compliant, rather than because they are being deliberately obtuse. It is important to constantly revisit the language used and seek to improve it, particularly as language is constantly changing in the way it is used in the information society. We have to be prepared to acknowledge that the solution to a consistent security finding may be a lot simpler than we first thought.

Governance

And finally, governance is the management of information within an enterprise, describing the overall management approach through which senior executives direct and control the entire organization, using a combination of management information and hierarchical management control struc-

tures. Governance activities ensure that critical management information reaching the executive team is sufficiently complete, accurate, and timely to enable appropriate management decision making, and provide the control mechanisms to ensure that strategies, directions, and instructions from management are carried out systematically and effectively. This should mean that we are providing our management teams with clear guidance and available metrics and measurements as to our security state, at any given time. Certainly this is often easier said than done, the more widespread an organization is. For example, as a consequence of so many security roles resting within IT functions, implementing Governance, Risk & Compliance (GRC) is often done from the point of rolling out the technology, without necessarily having the support and executive mandate required to address the intentions of the words and the principled performance improvement that were anticipated by the Open Compliance and Ethics Group (OCEG)[5] when they set out the GRC framework. For GRC to be effective, the entire organization needs to be working in harmony to achieve common goals and objectives while remaining in compliance with both legal requirements and societal expectations.

These are not opposite ends of a spectrum nor competing requirements – privacy cannot be achieved without security.

It's all about the process

In terms of structuring an internal security policy framework, there should be a hierarchy of activities, from an overall Security Policy Statement, agreed at the highest level, to a suite of Security Policies which address Security Requirements that are addressed through Control Standards. These, in turn, should be implemented across the organization through procedures that are workable whatever the circumstances. Finally, there are assessment procedures to ensure that everyone is doing what they are supposed to be doing in a way that achieves a measurement of security in a truly holistic manner.

However, just because we may have many standards addressing our ecommerce, credit card payment requirements, or our health care/privacy/data protection requirements or our public sector specific requirements does not automatically mean that they all have to be followed.

Not all controls are created equal.

Ira Winkler wrote about this most clearly in *Spies Among Us*.[6] He stresses that "countermeasures are never perfect," but that having them at least reduces the impact of incidents when they occur – and that really is the point of the exercise: selecting your controls (countermeasures) on the basis of a combination of risk assessment, knowledge of the organization, awareness of culture, risk, environment, cost, and political constraints as well as technological solutions available to you.

Most publications and authors articulate the approach to doing information security as requiring that you risk assess what it is you are seeking to protect or secure – information assets, systems, business processes, etc. – first, and only then, once you have identified risks that require some kind of "treatment," the business (system owners, etc.) needs to make a judgement about whether to accept, mitigate, or transfer the risks. Once a risk posture has been established, based on the risk appetite and tolerances of the organization, the necessary and appropriate controls can be selected to reduce the risks to an acceptable level that should be dictated by management. This can all be documented in a Risk Treatment Plan. You could equally reflect this end result in a Statement of Applicability, a statement of which controls are applicable for your situation; there is not an automatic assumption that ALL controls are relevant or necessary in ALL circumstances. The standards can all exist in isolation.

Seeing things more clearly

The available industry standards state what is required *if* a risk has been identified that needs an appropriate risk treatment to be applied. For many, there are cryptographic controls that will never be relevant. For some, there are information labelling and handling controls that will simply never be achieved for reasons of culture, budget, time, or resources. All of these stances are valid business responses, justifiable in any audit circumstance. It is for the business to decide how it manages its security posture, irrespective of how we, the security professionals, might wish it to be. Our job is always to provide the best advice and guidance possible; then write up the risks as and when we see them so there is at least some evidence of the right kind of thinking having gone on, should a breach occur.

Working with many teams over the years, I have seen that the ongoing increase in levels of compliance requirements seems to have led to a lack of focus regarding these key points. If time would only allow it, there really is a need to take stock, take a step back and reappraise the landscape to ensure that the implementation of controls is done systematically and with care for the resulting security as well as the efficiency to be gained from being pragmatic rather than check-box driven, an accusation often reflected at security and audit people who have objectives to evidence compliance requirements.

Does the mirror lie?

Perhaps due to pressures of workload or more likely in recent times due to shrinking resources, we have found ourselves with one set of compliance requirements being piled on top of another, rather than more sensibly being overlaid onto existing frameworks. If, for example, you take PCI DSS, read-

5 OCEG – http://www.oceg.org.

6 Winkler, I. (2005), *Spies Among Us*, Indianapolis: Wiley Publishing, ISBN: 0-7645-8468-5.

ing through the 12 key requirements of this standard, it is more than possible to overlay existing best practice information security requirements and the bulk of what needs to be done should already be being done. Thus, compliance with this particular standard need not be considered as a whole separate project in its own right, draining vast resources. If security best practice was being done as per the many requirements that have been made available over the years, at minimum the Sans Top 20[7] or the 20 Critical Security Controls for Effective Cyber Defense,[8] then achieving the objectives of many of these externally mandated requirements becomes much less of a challenge or a burden. The same can be said of achieving a balance between privacy and security requirements through the implementation of and adherence to mutually supportive controls. These are not opposite ends of a spectrum nor competing requirements – privacy cannot be achieved without security.

Seourity always gets in the way

Well, that's what we often hear, isn't it? But we security folk can often be the ones making a rod for our own backs. As a result of a decade of increasing regulation, legislation, and industry standard proliferation, we can risk finding ourselves so tightly bound in a level of complexity of process that we forget the actual purpose of embedding security controls, compliance, and governance. The framework is supposed to reassure everyone – our organization, our stakeholders, our clients, our customers – that we have everything under as much control as can be expected, given we are operating in an information society that is changing faster than ever before. This is made more difficult as we continue to operate on infrastructures that were not originally designed with security in mind, having to overlay them with a myriad of technologies in an attempt to plug the gaps.

Given the fast moving information society in which we are now operating, and the austere times that continue to surround us, we find ourselves having to unpick the complexity that has expanded with each iteration of regulation, legislation, standard, etc., challenging ourselves to streamline processes to something much more efficient and appropriate, while still delivering on the balancing act of achieving security and reducing risk. To work in security means having to understand a number of key fundamentals including that for us security means delivering on the promise of all three elements of the triad of confidentiality, integrity, and availability – but not *just* these three elements. It is all part of an interconnected system of inter-related concepts. Our systems thinking needs to be molded to suit the complex adaptive world in which we are now operating. We have no need to be building a new wheel every time a new piece of legislation is released, nor every time a standard is updated, or a new audit framework is released. We should be able to "map" our existing activities, show where they align, and carry on doing what

7 http://www.sans.org/critical-security-controls/

8 http://www.sans.org/critical-security-controls/winter-2012-poster.pdf.

we've been doing well – or better. There is clearly room for improvement, but duplication is definitely not appropriate.

Pulling it all together

Compliance is about checking whether what has been mandated or required in order to achieve security is being adhered to. Audit provides a valuable function in testing this. But we absolutely must work harder as a community of security professionals to pull together and combine our resources, knowledge, and expertise and scope our audits appropriately and then have the support of our management through their governance processes to address findings as and when they arise. Findings, observations, non-conformities (to standards, whether internal as required by the organization or external as mandated by industry or governing bodies) should not be the norm – they should be the exception. If we have written our policies, procedures, standards, and guidance properly and effectively enough to be followed by anyone stepping into any role across the organization, minimal findings should be our reality. No one should require constant security degree-level education to achieve the basics.

Conclusion

"We are living in challenging times." We are hearing this a lot these days. From an industry perspective, most organizations have been "doing" security for a long time now. I say "doing" because given the volume of ongoing breaches by large, public companies, the evidence is often hard to see. We should, by now, have a much deeper understanding of overlaps between the many available external standards to which we all need to comply to varying degrees. Therefore, our approach should be much more efficient. For many, this means having to look to changing the approach and really starting to behave in a leaner way. Repeatable and transferable controls are what we should be aiming for in order to achieve the best metrics, measurements, and quantifiable results. Our documentation must be intelligible and our evidence must be clear. Our use of terminology needs to be consistent in order to successfully deliver on the linked concepts of standards, compliance, and governance. If we are going to continue to use these terms, we really must endeavor to live up to their actual meanings.

Recommended Readings

Blyth, A.J.C. and Kovacich, G.L. (2006) *Information Assurance – Security in the Information Environment*, 2nd edition, London: Springer-Verlag, ISBN 1-84628-266-7.

Boyce, J.G. and Jennings, D.W. (2002) *Information Assurance: Managing Organizational IT Security Risks*, London: Butterworth Heinemann, ISBN 0-7506-7527-3.

Herrmann, D.S. (2002) *A Practical Guide to Security Engineering and Information Assurance*, Auerbach Publications, Florida: CRC Press, ISBN 0-8493-1163-2.

MindfulSecurity.com, What are Policies, Standards, Guidelines and Procedures? – http://mindfulsecurity.com/2009/02/03/policies-standards-and-guidelines/.

Peltier, T.R. (2001) *Information Security Risk Analysis*, Florida: CRC/Auerbach Publications, ISBN: 0-8493-0880-1.

—(2002) *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*, Florida: CRC/Auerbach Publications, ISBN: 0-8493-1137-3.

—(2004) *Information Security Policies and Procedures: A Practitioner's Reference*, Second Edition, Florida: CRC / Auerbach Publications, ISBN: 0-8493-1958-7

Schou, C. and Shoemaker, D. (2007) *Information Assurance for the Enterprise: A Roadmap to Information Security*, New York: McGraw-Hill Irwin, ISBN 10: 0-07-225524-2 / ISBN 13: 978-0-07-225524-2 / ISBN-13: 978-0-07-225524-9.

Wylder, J. (2004) *Strategic Information Security*, Florida: CRC/Auerbach Publications, ISBN: 0-8493-2041-0.

About the Author

Andrea C. Simmons, FBCS CITP, CISM, CISSP, M.Inst.ISP, MA, ISSA Senior Member, is currently Global Head of Policy Governance for HP Enterprise Security Services, providing key strategic management insight across both the security policy function as well as addressing the metrics and measurement of security to enhance an organizations posture and profile. Andrea has just completed her second book, Managing Information Security, addressing the role of the Information Security Manager across a 12-month span. Andrea is also a part-time PhD research student at the University of Wolverhampton, studying Information Assurance in depth, from the point of view of its meaning and usage, in particular across the public sector. She may be reached at andrea.simmons@bcs.org.

Figure 82: Simmons (2012b)

10.10 PhD Annual Review Poster 2011

UNIVERSITY OF WOLVERHAMPTON
KNOWLEDGE • INNOVATION • ENTERPRISE

Redefining Information Assurance for the UK Public Sector

Andrea C Simmons, MA, CISM, CISSP, FBCS CITP, M.Inst.ISP

BACKGROUND – What is the case?

Definition of Information Assurance (IA) 'Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.' NSTISSI 4009, August, 1997

Information Assurance is the confidence that the information assets within an organisation are reliable, accurate, secure and available when required. Thus, Information Assurance is the protection of information and information systems by ensuring their integrity, authentication, confidentiality and non-repudiation

PURPOSE – What are the implications?

So if that's the definition, why are we still having data breaches and information losses on increasing scales, with a lack of improvement that reflects badly on the professionalism of the industry.

The challenge is to research why it is that we have spent at least a decade explaining Information Assurance at Director Level, and yet still have a lack of understanding at senior management level and a lack of buy-in and adoption to deploying best practices and embracing thorough information risk management where information assets are afforded the same corporate protection as other assets.

AIMS

The aim of this research is to highlight the already existing volume of available material, through reviewing it critically, reflecting on the historical, political, cultural, economic and other contexts which make sense of it.

In the context of this research, the focus is on the intersection between central and local government – so the outputs will provide all public sector employees, all civil servants, permanent secretaries and the relevant MPs etc – with tangible, implementable frameworks and guidelines to embed Information Assurance as was always intended, or to show where its ultimate journey should lead them towards – ***Information Governance***.

The desired personal goal would be to end up as a Chief Scientific Advisor to the Government on Information Governance for the next term of office, 2015.

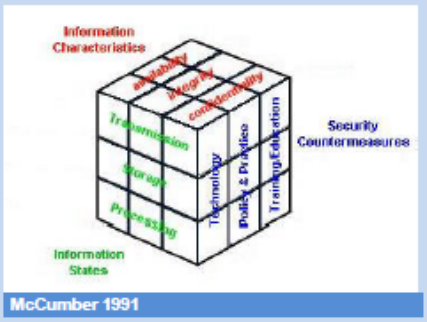
METHODOLOGY

The methodology is a combination of the following:
- Drawing inspiration from the ethnomethodological critique of government and industry reports and similar documentary sources,
- Addressing the haecceity and quiddity of Information Assurance - just what makes it what it is, including the origins of its definition, beyond that of Information Security?
- Content analysis of documents encountered
- Recording of observations
- Participatory action research, observing and detailing illustrative incidents
- Reflexive Ethnography – production of knowledge

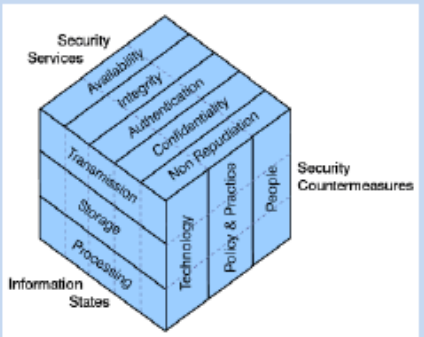
CONTRIBUTION

A book has already been published provide reference to best practice in Information Security (December 2008) ***Achieving Best Practice in Public Sector Information Security, Ark Group Publishing, ISBN 978-1-906355-39-5***

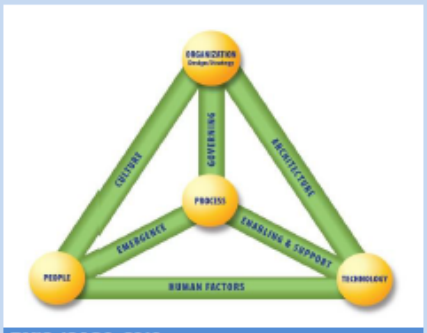
This is to be followed up with another book currently entitled "**Once more unto the breach; a year in the life of an Information Security Manager**" highlighting information loss and data breach incidents and lessons learnt.



McCumber 1991



Maconachy 2001



BMIS, ISACA, 2010

Areas to be explored:
- Management Theory
- Systems & Interdependence
- Organisational Culture
- Ethics & Professionalism
- The impact of Politics

andrea.simmons@bcs.org, 07961 508775

Figure 83: PhD Annual Review Poster 2011

10.11 PhD Annual Review Poster 2013

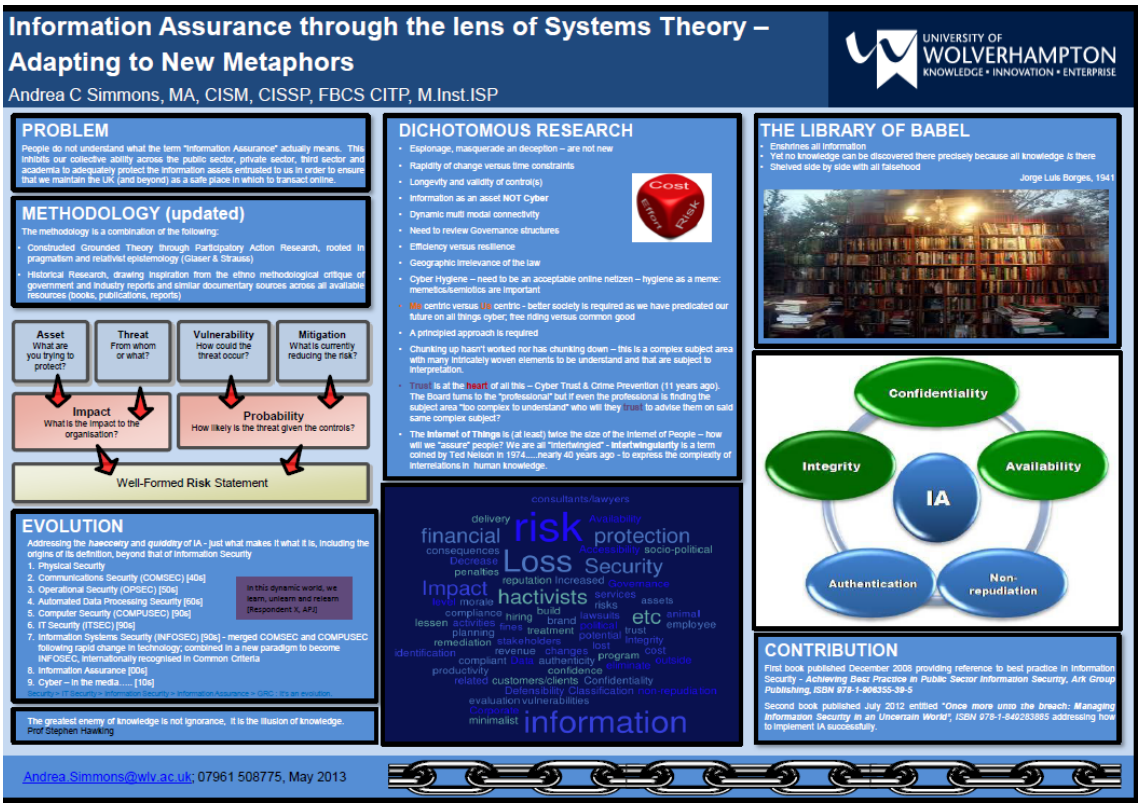


Figure 84: PhD Annual Review Poster 2013

10.12 PhD Annual Review Poster 2014

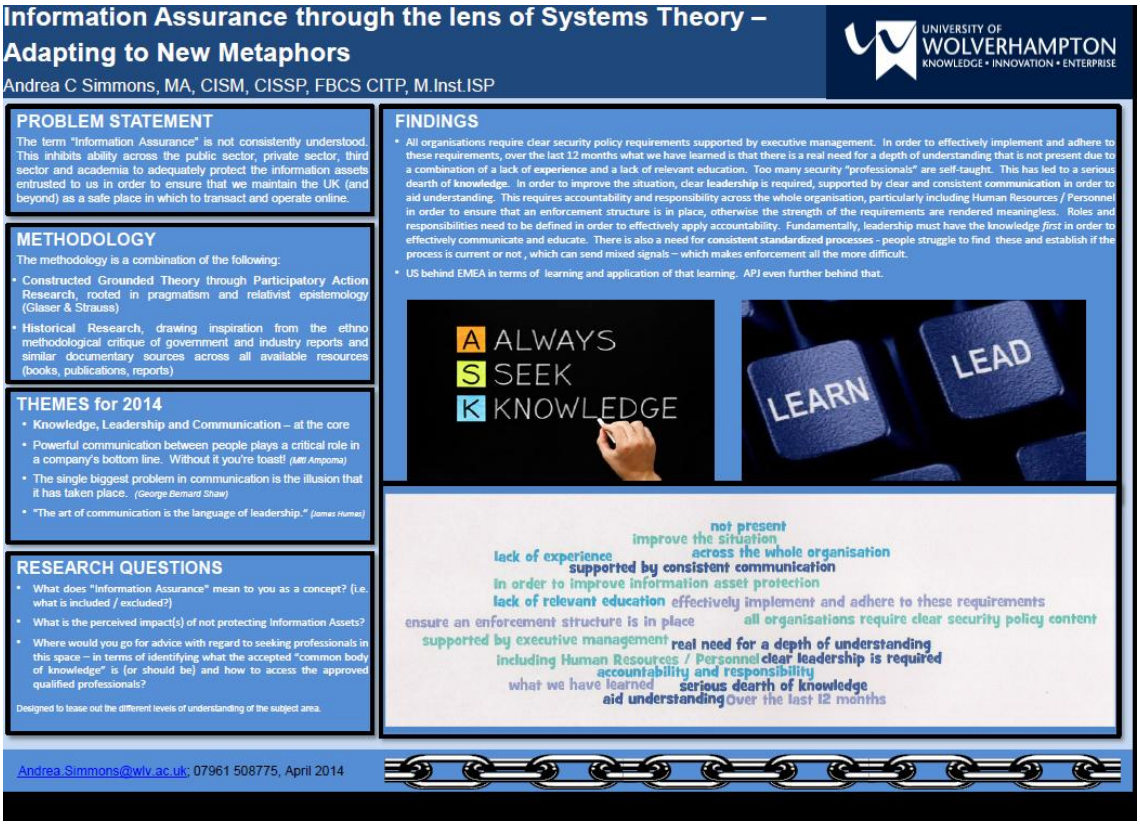


Figure 85: PhD Annual Review Poster 2014

10.13 PhD Annual Review Poster 2015

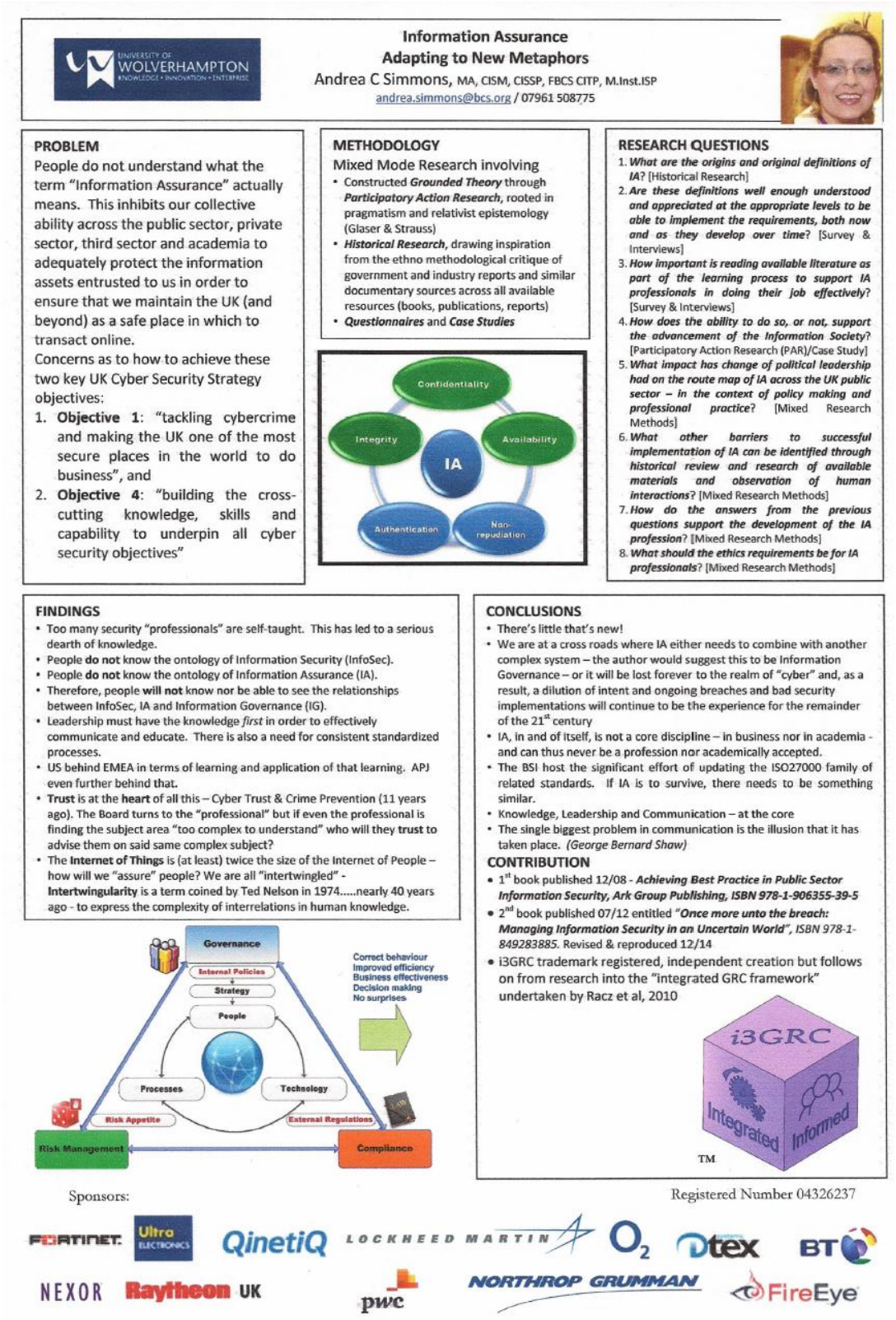


Figure 86: PhD Annual Review Poster 2015

10.14 IAAC Review Questionnaire 2010

Information Assurance

A Review

What does IA mean to/for you and how has this changed?

"IA – valuing and protecting information"

IAAC has been fundamental to shaping the IA agenda and thinking during the last decade. Our last in depth analysis of understanding and attitudes towards IA took place in 2002. Revisiting the topic in this way should garner lessons learnt from experiences during the past eight years. This will help to ensure that the UK Information Society encompassing Government, Private Sector and the Individual enjoys an information environment that is robust, resilient and secure for the 21st Century.

Overview

1. If possible, can you remember when you first heard the term "IA" used?
2. What does "IA" mean to you as a concept? (i.e. what is included / excluded?)

Terminology

2. How long (if at all) have you been using "IA" as a term in your organisation?
3. Is the term IA useful in your organisation (in terms of winning hearts and minds and changing behaviour, if required)? If not, what is a better term for businesses and other operational organisations to use?
4. Further to question 4, has your organisation changed its terminology over the last decade and, if so, what terms have been used, when and why were they changed?

Drivers and Obligations

5. To the best of your understanding, how different are public, private, academic and third sectors in meeting IA legislative, regulatory, statutory and standard compliance objectives? *Expand.*
6. What is the perceived impact(s) of not protecting Information Assets?
7. Has your Board prioritised IA activities appropriately to address current information risks?
8. Lower insurance premiums would be a significant factor for encouraging the adoption of best practices in IA – agree/disagree/ discuss:

Standards and Measurements

9. Is there a particular IA/InfoSec/IT standard that dominates your organisation's IA policy?
10. How do you measure the benefits of compliance with these standards (i.e. using particular metrics, key performance indicators [KPIs] etc)?
11. How do you measure the benefits of IA (i.e. maturity modelling)?

Impact of Culture and Politics

12. Would you say that changes in the **political landscape** have had an impact (either positive or negative) in terms of the ability of either a public or private sector body to deliver their respective services? *Explain/elaborate*.
13. Expanding on your thoughts/response to question 6, what impact (if any, positive or negative) has changes in **public sector culture** and attitude towards information assurance had on the abilities of the public sector, sub-contractors, clients and customers to protect information assets appropriately?

Professionalism of ICT and IA

14. To what extent has the progression of professionalising the industry (both ICT and IA) impacted positively (or negatively) in terms of embedding the requirements of IA within the relevant roles and organisational structures? *Explain*
15. Where would you go for advice with regard to seeking professionals in this space – in terms of identifying what the accepted "common BoK" is (or should be) and how to access the approved qualified professionals?

10.15 Private Sector Review Questionnaire 2012

What does Information Assurance mean to/for you and how has this changed over time?
"IA – through the lens of Systems Theory"
We are constantly hearing about a "cyber skills crisis" these days. The central premise of this PhD research is that if we better understood the fundamentals of information assurance (IA) and its journey from computer security, through IT security to InfoSec and thence to IA, we would have a clearer perception of reality that holds less of a "crisis" and more of a need to engage with the many professionals already working hard across the industry. IA is not yet fully accepted as an academic discipline so we have a way to go in explaining what it's all about. Applying Systems Theory to it helps to think through the various component parts of what actually makes up IA and review them appropriately. I would be very grateful if you would please complete the questionnaire below and be part of that educational process to improve the landscape for us all.
Overview 1. If possible, can you remember when you first heard the term "IA" used? *2.* What does "IA" mean to you as a concept? (i.e. what is included / excluded?)
Terminology 3. How long (if at all) have you been using "IA" as a term? 4. Is the term IA useful in your area/team/section/group….? If not, what is a better term to use? 5. Further to question 4, have you changed terminology usage over the last decade and, if so, what terms have been used, when and why were they changed?
Drivers and Obligations *6.* How different are public, private, academic and third sectors in meeting IA legislative, regulatory, statutory and standard compliance objectives? (i.e. from *your* perspective, what differences do you see in client understanding of the issues) *Expand.* 7. What is the perceived impact(s) of not protecting Information Assets? 8. How do you measure the benefits of IA? 9. Lower insurance premiums would be a significant factor for encouraging the adoption of best practices in IA – agree/disagree/discuss (i.e. would clients use this option and would it really help?):
Standards and Measurements 10. Is there a particular IA/InfoSec/IT standard that dominates your IA approach? 11. How do you measure the benefits of compliance with these standards?

Impact of Culture and Politics

12. Would you say that changes in the **political landscape** have had an impact (either positive or negative) in terms of the ability of either a public or private sector body to deliver their respective services? *Explain*.
13. Expanding on your thoughts/response to question 6, what impact (if any, positive or negative) has changes in **public sector culture** and attitude towards IA had on the abilities of the public sector, sub-contractors, clients and customers to protect information assets appropriately?

Professionalism of ICT and IA

14. To what extent has the progression of professionalising the industry (both ICT and IA) impacted positively (or negatively) in terms of embedding the requirements of IA within the relevant roles and organisational structures? *Explain*
15. Where would you go for advice with regard to seeking professionals in this space – in terms of identifying what the accepted "common BoK" is (or should be) and how to access the approved qualified professionals?
16. If you were to recommend one good, informative, educational book to a new Account/Privacy Security Officer to read, what would it be?

10.16 Research Demographics

Table 20 provides the demographics for participants in both survey research and semi-structured interviews, coded as follows:

E = Email correspondence
ES = Survey respondent with extra email input and conversational follow-up
ESk = Emails and Skype semi-structured interview
F = Face-to-Face semi-structured interview
FE = Face-to-Face semi-structured interview and email follow-up
FS = Face-to-Face semi-structured interview and survey completion
S = Survey respondent
T = Telephone semi-structured interview
Te = Teleconference with global private sector clients, i3GRC™ explained

Code	Sector	Respondent Type	Respondent Area	Where	How
1F	Academia	Lecturer	Industry expert	UK	Face-to-face
2F	Private	Consultant	InfoSec Professional	UK	Face-to-face
3F	Private	Consultant	IA Practitioner	UK	Face-to-face
4T	Private	Consultant	Forensic specialist	UK	Telephone
5F	Private	Consultant	IA Practitioner	UK	Face-to-face
6F	Private	Consultant	IA Practitioner	UK	Face-to-face
7ES	Private	Consultant	Politics	UK	Email and Survey
8E	Government	Practitioner	CSIA (as was)	UK	Email
9E	Private	Consultant	Private Sector Outsourcing (Consulting)	UK	Email
10FS	Government	Practitioner	Defence, MOD	UK	Face-to-face and Survey
11E	Private	Lawyer	Legal	UK	Email
12E	Private	Consultant	InfoSec Professional	UK	Email
13F	Public	Practitioner	The National Archives	UK	Face-to-face
14F	Government	Consultant	Ex military	UK	Face-to-face
15ES	Private	Consultant	Industry SME (Smart Cards)	UK	Email and Survey
16FS	Private	Consultant	IA Practitioner	UK	Face-to-face and Survey
17E	Private	Consultant	InfoSec Professional	USA	Email
18E	Academia	Practitioner	Academia	UK	Email
19F	Private	Consultant	InfoSec Professional	UK	Face-to-face
20F	Academia	Lecturer	IA Practitioner	UK	Face-to-face

Code	Sector	Respondent Type	Respondent Area	Where	How
21E	Academia	Lecturer	Academia, IAAC	UK	Email
22F	Private	Practitioner	EU Skills Agenda	Ireland	Face-to-face
23F	Private	Consultant	Cyber Security KTN (as was)	UK	Face-to-face
24T	Public	Practitioner	London Met Police	UK	Telephone
25E	Private	Professional body	Information Records Management Society (IRMS)	UK	Email
26F	Public	Practitioner	CESG	UK	Face-to-face
27E	Private	Professional body	(IISP	UK	Email
28T	Private	Practitioner	Cyber Security Champions	UK	Telephone
29E	Government	Practitioner	National Infrastructure Security Co-ordination Centre (NISCC)	UK	Email
30E	Private	Consultant	InfoSec Professional	UK	Email
31ES	Private	Consultant	InfoSec Professional, consulting	UK	Email and Survey
32ESk	Academia	Lecturer	InfoSec Professional	UK	Email and Skype
33Te	Private	Practitioner	InfoSec Professional	USA	Teleconference
34F	Private	Practitioner	Software Management – Security Assurance	USA	Face-to-face
35F	Private	Consultant	ISO 27001 Expert	USA	Face-to-face
36Te	Private	Practitioner	Large global payments business	USA	Teleconference
37Te	Private	Practitioner	“Big 4”Audit Firm (A)	USA	Teleconference
38E	Private	Practitioner	InfoSec Professional	USA	Email
39FE	Private	Practitioner	InfoSec Professional	USA	Face-to-face and emails
40Te	Private	Practitioner	CIO, Worldwide Travel company	USA	Teleconference
41E	Private	Practitioner	GRC Professional (A)	USA	Email
42E	Private	Practitioner	GRC Professional (B)	USA	Email
43F	Private	Practitioner	“Big 4” Audit Firm	USA	Face-to-face

Code	Sector	Respondent Type	Respondent Area	Where	How
44F	Private	Practitioner	“Big 4 Audit Firm (B)	UK	Face-to-face
45S	Private	Practitioner	InfoSec Professional, Healthcare	USA	Survey
46S	Private	Practitioner	InfoSec Professional, retail	USA	Survey
47S	Private	Practitioner	InfoSec Professional	Australia	Survey
48S	Private	Practitioner	InfoSec Professional	Australia	Survey
49S	Private	Practitioner	InfoSec Professional	UK	Survey
50S	Private	Practitioner	InfoSec Professional, Healthcare	USA	Survey
51S	Private	Practitioner	InfoSec Professional	USA	Survey
52S	Private	Practitioner	InfoSec Professional	UK	Survey
53S	Private	Practitioner	InfoSec Professional	USA	Survey
54S	Private	Practitioner	InfoSec Professional	Ireland	Survey
55S	Private	Practitioner	InfoSec Professional	UK	Survey
56S	Private	Practitioner	InfoSec Professional	UK	Survey
57S	Private	Practitioner	InfoSec Professional	Singapore	Survey
58S	Private	Practitioner	InfoSec Management	Australia	Survey
59S	Private	Practitioner	InfoSec Policy leadership	USA	Survey
60S	Public	Practitioner	IA Practitioner	UK	Survey
61S	Public	Practitioner	CESG	UK	Survey
62S	Public	Consultant	Ex military	UK	Survey
63S	Public	Consultant	Ex military	UK	Survey
64S	Public	Practitioner	IA Practitioner	UK	Survey
65S	Third	Practitioner	IA Practitioner	UK	Survey
66S	Academia	Practitioner	IA Practitioner	UK	Survey
67S	Private	Practitioner	IA SME Consultancy	UK	Survey
68S	Private	Consultant	Independent IA consultant	UK	Survey
69S	Public	Practitioner	IA Practitioner	UK	Survey
70S	Private	Consultant	Independent IA consultant	UK	Survey

Code	Sector	Respondent Type	Respondent Area	Where	How
71S	Public	Practitioner	National Health Service (NHS)	UK	Survey
72S	Public	Practitioner	IA Practitioner	UK	Survey
73S	Public	Practitioner	IA Practitioner	UK	Survey
74S	Private	Consultant	Independent IA consultant	UK	Survey
75S	Private	Practitioner	Military	UK	Survey
76S	Government	Practitioner	IA Practitioner	UK	Survey
77S	Government	Practitioner	IA Practitioner	UK	Survey
78S	Government	Practitioner	Local, IA Practitioner	UK	Survey
79S	Government	Practitioner	IA Practitioner	UK	Survey
80S	Public	Practitioner	IA Practitioner	UK	Survey
81S	Government	Practitioner	Leeds CC, IA Practitioner	UK	Survey
82F	Public	Practitioner	Healthcare professional	UK	Face-to-face
83F	Private	Practitioner	Manufacturing professional	UK	Face-to-face
84F	Private	Practitioner	InfoSec professional	UK	Face-to-face
85ET	Government	Practitioner	InfoSec professional	UK	Email and Telephone
86F	Government	Practitioner	InfoSec professional	UK	Face-to-face
87F	Government	Practitioner	InfoSec professional	UK	Face-to-face
88ES	Private	Practitioner	InfoSec professional	UK	Email and Skype
89ET	Academia	Practitioner	InfoSec professional	UK	Email and Telephone
90ET	Private	Practitioner	InfoSec professional	UK	Email and Telephone

Table 20: Research Demographics

10.17 Survey Memos

The following are respondent comments taken from the Questionnaire returns and Interviews which have been utilised in the discourse analysis.

Terminology

Code	***Response commentary***
5F	*IA is an expansion of the InfoSec discipline*
6F	*IA fairly new in 2002*
10FS	*It's a philosophy – need to tolerate risk and highlight the value of risk taking* *Level 1 = personal data* *Level 2 = business critical data* *Level 3 = robust*
10FS	*Do IAOs actually look after data? Culture change plan*
10FS	*Much more focus on information – have an IM Strategy*
10FS	*For traction / prominence / focus – then risk management*
10FS	*Cyber defence / Cyber security / Cyber attack - 3 way*
10FS	*Challenging ambiguity in an area of no clarity*
10FS	*The higher you get the less you know*
10FS	*Requires gravitas, confidence*
10FS	*Interdepartmental InfoSec officers, proactively adapting governance policy*
10FS	*IA delivery group in Cabinet Office (under John Suffolk) – John Taylor runs it at MOD as SIRO*
10FS	*Putting it in job contract*
10FS	*Not techies*
10FS	*Stakeholder Management = a key skill*
10FS	*Generalist / breaking down complexity*
10FS	*£600m to be spent on cyber security – IA being subsumed into this….*
10FS	*Training delivered internally*
10FS	*DPO/FOI separate from IA, at the MOD*
10FS	*I believe the MOD has used the term InfoSec in the past* *It also uses Operations Security, but this use is confined to all types of security pertaining to a combat operational setting.*
10FS	***Observations:*** *IA can be good and yet Records Management not yet implemented….short sighted and not in IG mode*
15ES	***Included****:* *CSIA defines IA as the confidence that IS will:* • *protect the information that they handle;* • *function as they need to, when they need to; and* • *be under the control of legitimate users.* *(Ref: IA: A review of UK Government and industry initiatives, Nick Coleman for CSIA, Oct 2004, page 6)* ***Excluded****: clear legal requirement for public sector bodies and private sector organisations to get it right.*
15ES	*…. outside core critical national infrastructure areas, the whole IA push has failed, but you don't ask for comments at that level. So here is one: large sections of the civil service do not operate in the fact driven environment that we have to inhabit in the commercial and related environments (e.g. professional, academic) - and we cannot force them to change, because they are a third but unaccountable power in the country: elected representatives, appointed government, civil service. Local Govt largely follows in the wake of the civil service. So IA doesn't translate into many areas, but InfoSec does for those organisations that realise they must take the topic seriously as an extra component of ICT in their already well developed corporate governance strategy. A final note: CESG and GCHQ only provide advice in many areas, advice that can be and, it seems, is often ignored.*

15ES	*Have introduced both IA and InfoSec. IA has no impact. Have introduced the terms because (a) we previously assumed that professionalism would ensure that all involved would take InfoSec into account (but increasing threats meant a more formal approach), and (b) I naively hoped that IA concepts would drive the public sector to become much more competent (but, in the areas where we are involved, it didn't).*
31ES	*It's an umbrella term covering all the areas that can impact or effect the (overall) assurance that can be ascribed to information, i.e. how available is the information, how much confidence can we put on the integrity of the information and how confident are we that the information can only be accessed/used by authorised people or processes. As such IA covers risk and threat analysis (business, technical and physical), system "fit for purpose" analysis, development and deployment of risk mitigation controls and regular auditing to ensure that the controls are both fit for purpose and effectively implemented, and in regular use. Training, policies, procedures, and guidance are outputs from the IA process.*
35F	*Inconsistent and ill-informed / ill-educated Interpretation of security terms is at the heart of the issue*
48S	*IA is risk management programme (identification, evaluation, treatment of risks) against the unauthorised access, use, corruption, loss or disclosure of information assets. A positive way to present IA is to ensure that the right information is provided to the right Actors with the correct business justification for access, at the right time and in an auditable/trackable way.*
50S	*"IA" is likely to be confused with "Quality Assurance" which itself seems to have different meanings for different people, even within a single software development organisation.*
50S	*My understanding of the scope of InfoSec has changed over the past decade. Previously I did not associate InfoSec with "availability" in the sense that DR activities would be of interest to a security professional. Additionally, I viewed "integrity" in the narrow sense of preventing unauthorized changes to data.*
53S	*What is in place to protect information based on their value (physical and digital) and how leaders are planning, action, and response that could lessen or eliminate related vulnerabilities?*
53S	*Cloud is introducing interesting approach with IA and IA Framework that provides set of questions that an organisation can ask cloud providers to assure themselves that they are sufficiently protecting the information entrusted to them and allow direct benchmark based somewhere to IA*
54S	*I think apart from the obvious changes in some technical terminology due to technology shifts, data, IM and the intelligence gained from information is now clearly seen in the main stream as a business asset more so than that stuff that sits in a file share or reside in a database. There is a greater need to understand what to protect and how to strategically safeguard it. Information is tangible asset that needs to be managed and can be assigned dollar value. Where in the past I think in IT we were more concerned with the underlying infrastructure of services but not necessarily the data that actually flowed through out those piece of infrastructure. Many terms relating to data have evolved due to heavy regulation, data privacy and the wakeup call to the C level executives that found they were being sent to jail due to the fact they were not protecting their organisations, customers and employees data.*
54S	*The term IA means to me as a concept is that the use of the data and where it resides is managed protected and the availability of the interconnected systems that house this information has appropriate controls and safe guards in place. I think it also includes data classification, knowing the levels of protection that should be applied to the organisations data and understanding the threats levels and management of risk needed to ensure CIA.*

57S	*I was in a SANS Seminar in 1999 and that is where the tem **"InfoSec"** was clearly articulated. InfoSec covers protection of information received, created, processed and stored within/through people, technology (computers, applications and data and also physical documents/records.* *I first heard of IA term from my US colleagues while I was seconded to work on government outsourcing project. These colleagues have worked on the US government defence projects.*
57S	*….in this dynamic world, we learn, unlearn and relearn. Based on this philosophy, I have been involved in all domains of InfoSec (ISO 27001:2005) covering security architecture, policy, risk assessment, security project implementation, managed security services and compliance/audit/assessment.*
57S	*In broad terms, **IA** is to build the confidence in the stakeholders of using the information provided and therefore have **trust** in the information residing in the systems and physical documents.*
57S	*IA to my understanding is the outcome of the security programmes and activities to build trust and confidence in using IS.* *a. It is a process whereby all the elements of risk associated with information (CIA, etc) are managed* *b. It includes "responsible" IM and information exploitation; it includes network defensive measures and physical and human measures to provide appropriate protection to the information to enable it to be used for the business/operational purpose* *c. It excludes IO and the use of information as a weapon*
57S	*Initially when I came across the terms, my understanding was superficial and did know how much I did know. Over the years doing consulting and implementation work for clients, my understanding has deepened and appreciates the intent and purpose of the terms.*
57S	*ISF defines "Assurance is providing evidence to someone that something is working as required."*
59S	*IA is the practice of protecting "securing" all assets and managing the risks associated; whether transmitted or stored electronically, physically or handled through administrative procedures.*
62S	*IA is an all embracing term. True IA means that I can rely on what I am seeing and reading whether on a packet of frozen food in the supermarket, an warning sign on a motorway or an e mail from my bank.*
65S	*I do not believe the term IA is helpful to people who do not have a background in either secure systems or IA.*
60S	*IA is about managing the quality and security of information. It is one part of information governance.* *Problem of overlapping definitions with 'information governance', 'information quality' and 'InfoSec' – which are all terms that I use regularly in preference to 'information assurance'*
68S	*IA is based on a governance process which is designed to provide assurance that an organisation's data is protected in terms of Confidentiality, Integrity and Availability. It is most commonly mapped against ISO 27001 controls and reporting.*
69S	*IA was "InfoSec" and changed to reflect demands of public sector.*
71S	*In the NHS we tend to use IG much more than IA.* *Our specialist group in BCS is called IRM and Assurance however there is a rumbling going on about possibly changing the name to IG. This has much more resonance when considered alongside Corporate Governance, Fiscal Governance and in the NHS Clinical Governance.*
72S	*Seems odd that Private and Public sectors use differing words for the same meaning!*
73S	*The term has only recently been adopted (2009) but is only known to a small subset of teams/individuals with the organisation. However it is used more when dealing with third parties where a relationship currently exists.*

74S	*If InfoSec is about helping to stop bad things from happening, then IA is about helping to ensure that good things happen. It includes InfoSec, i.e. if bad things happen then good things aren't happening, and includes strengthening those attributes of information that make information an asset for the organisation. So, if the organisation needs some of its information to be accurate, then IA includes steps to improve the accuracy of that information, if it needs some of its information to be current to the second (as in trading desks) then IA includes steps to reduce the latency in gathering that information, if it needs some information to be available to anyone on demand, then IA includes steps to improve the discoverability of, and access provided to, that information.*
75S	*CIA - In current academic role: I don't think academics know what any of these terms mean. Peer Review? Huh.*
77S	*IG is the term which seems to be emerging at the moment merging IA, Knowledge Management, IM and IT into a consistent risk based approach.* *A better term is IG when placing it in a business risk management context.*

Table 21: Terminology - Coded Respondent Commentary

Drivers and Obligations

Code	***Response commentary***
10FS	*All sorts of potential consequences: financial costs, legislative penalties, cost to life in operational settings and most often reputational penalties to the organisation*
10FS	*It can also have consequences to the individual, especially in respect of loss or identity or fraud.*
15ES	*Public sector organisations that I encounter take no constructive notice until hit by the ICO – even then they are not fully embracing the requirements. Private sector tries much harder but is prepared to take risks.*
31ES	*There is a general failure of understanding the regulatory, statutory and standard compliance objectives though there are the odd beacons of understanding. Security controls are often added in as an afterthought, also security controls are often seen as a hindrance to doing business. These two statements go hand in hand.*
31ES	*It depends on the client. It could be just loss of reputation (a data loss splashed across the newspapers) or it could be loss of business (a competitor gets the client list and poaches clients or learns of a new product and brings their own to market first) or both (retailer losing customer credit card records, reputational damage plus customers leave and potential new customers shies away from the retailer).*
45S	*Increased cost (remediation activities, hiring of outside consultants/lawyers, etc.), potential financial consequences*
45S	*Loss of productivity*
45S	*Decrease employee morale*
46S	*Loss of intellectual property*
46S	*From my experience, it depends on the nature of the company. Public sector organisations tend to have quite a lot of control requirements around IA. For example many have to follow specific regulations and/or security requirements around protection of data and systems. Service providers to these public sector organisations may also have to become accredited in order to provide services and be regularly audited to ensure they are meeting the accreditation requirements.*
46S	*Private sector companies tend to be a bit more hit and miss. It seems to depend on the nature of the business they are doing as to how much attention they pay to IA or "Security" as it is usually referenced. Companies in the banking and finance industry naturally pay a lot of attention to IA given the type of personal data they are handling. Manufacturing companies tend to be a lot more lax in this area and seem to work under the misguided belief that no one would want to "hack" their organisation. About the only area that gets any attention is any online transacting they may be doing otherwise it is very difficult to get mindshare around IA.*
46S	*I think this is quite hard. Often there is no tangible benefit that you can measure. It's pretty hard to measure not being attacked, not losing data and no brand damage. You could potentially use Audit results, reports from tools that have been used to perform risk assessments, IPS/IDS reports, Firewall reports etc.*

46S	*Insurance - I don't think it would be a beneficial way to look at implementing IA as it's about more than just a reduced premium.*
47S	*Impact on delivery of services to customers/clients*
47S	*Animal hactivists / Political hactivists*
47S	*Socio-political changes*
48S	*There aren't a lot of IA legislative requirements in Australia outside of Government – apart from some pretty weak privacy laws.*
48S	*Public Sector puts a lot of strength in the "need" to be compliant but there is generally lip service to the actual execution of compliance unless there is an audit or some other level of personal (and visible) accountability. When this public visibility risk is realised, then it is all hands to the pump to become minimalist compliant as soon as possible.*
48S	*In Australia, mostly reputational – but in saying that there are penalties for large data privacy losses – but the penalties are not readily applied – case in point was that Australia's largest carrier exposed the data of their 700,000 customers but avoided penalty: http://www.theaustralian.com.au/business/breaking-news/telstra-avoids-fine-for-privacy-breach/story-e6frg90f-1226490650522*
49S	*The different objectives / end goals and to a certain extent, resources of public, private, academic shape their focus on InfoSec. Based on previous experience, it depends on which industry that the client falls under. Their willingness / openness to invest resources will vary according to these objectives / end goals. For instance, where private agencies are concerned, their perspective might be to maximize InfoSec based on a minimal investment of resources whereas public agencies might invest more than what conventional risk management wisdom would dictate.*
50S	*The client's senior staff seems to have limited awareness of the ethical and legal implications of protecting PHI and PII, and generally seems to treat even basic security practices (e.g., wearing photo ID badges while in a facility where most staff have access to sensitive information) as a nuisance (US Healthcare).*
51S	*Financial Institutions more concerned than Industrial Companies*
56S	*Well, all above sectors are very different per realm and will be used very specifically in very different client environments and so all clients understand them also as an important way to protect their own company/client information, assets and products.* *They are using their own window to have an appropriate outlook to their own specific area and the specific way to protect these (standards, regulatory …).* *They all are focused on the legal and industry specific requirements and they are very concentrated to follow their general objectives related to all of these requirements.* *Therefore we will have a very high potential grade of investment chances in our future business life.*
56S	*To run in massive business and important intellectual business properties casualties.* *To lose trust and reputation on the market and as a result of this you run in unforeseen company turbulences.* *All of that makes it worth to invest finally in SECURITY products to protect all company assets and don't lose the capital of the firm.*
57S	*Legal implications*
57S	*From a security professional point of view, working for government security projects is demanding but also enlightening. One is challenged on all types of security issues and need to articulate/justify your actions to have trust and confidence in your initiatives.*
57S	*Next is the banking sector where the stress is more on compliance first and then security risk management.*
57S	*Third group is companies that need to comply with regulations like SOX or have to meet the standards to meet certification requirements like ISO 27001:2005.*

58S	*Projects for government clients include stringent requirements for InfoSec covering people, technology and processes. Government clients lay emphasis and demand the best security, sometime going beyond the balance of security and risk.*
58S	*Based on the wide variety of customers that I have worked with in the past two decades this varies quite a bit. I find that public/academic sectors are well ahead of many private institutions. Seems that they have the attitude of everything is okay so let's spend the money elsewhere.* *I also believe that many leaks that have been reported are much higher for private sectors. Well it certainly appears that way. I even estimate that 65-80% are still at risk.*
58S	*This can range from exploitation, fraud, disruption and information disclosure and can in many cases causes un-repairable damage to reputation and in some cases complete loss of business. Confidence in public sectors will be severely impacted.*
58S	*Appropriate implementation of monitoring and reporting tools is a first major step. Management will not spend money mitigating risks unless some measurable benefit is shown. In many cases, management will reduce funding where inappropriate reporting has been implemented. It's important to keep management aware of the types of issues that occur and that they have been dealt with appropriately. It's also important to show the cost benefits*
63S	*IA is seen by some as something Zealots talk about!*
63S	*Because process is more prevalent in Public Sector, there is more visible adherence to IA. Private Sector, especially manufacturing, is less process focused; as a result, IA is less evident.*
65S	*I suggest that public organisations follow the rules laid down by their senior masters – i.e. Perm Secs or Cabinet Office central teams. The private sector do what they need to avoid litigation and to sell products and services – if the requirement states certain IA objectives have to be met then they will meet them, but not always in a voluntary way. I imagine academic organisations have centres of excellence where IA is taken very seriously but they will be exceptions. The Curate's egg comes to mind. The third sector is surprisingly variable but this is probably because of poor leadership from HMG and Whitehall. When the Minister for Digital Access and Inclusion and his core team do not does know that the Disability Discrimination Act (DDA) is law what hope is there for IA in the 3rd sector? In AbilityNet we take IA very seriously at all levels as we deal with some of society's most vulnerable people. This is however an uphill struggle with little help from HMG at the present time. Even the UK's Digital Champion is only interested in getting 10 million people on line – but not on line safely.*
65S	*….but more leadership across Whitehall would be useful – having done their bit on lost IT equipment and sensitive documents they appear to have lost interest in helping the general population. To some of my colleagues IA was seen as an activity by HMG to protect its own secrets rather than helping the public. I have to say they had and still have my sympathy for taking such a polarised view.*
67S	*The compliance objectives that seem to work are those where the regulations have some effective penalty (such as SOX and PCI DSS). This makes the impacted organisations (typically private sector and third party suppliers) take positive action. The US has more compliance objectives that includes an effective penalty. Bad press certainly causes reputational damage which impacts third party supplier but does not seem to impact public sector organisations The public sector takes action only because they could end up with a 'bad report' and typically they are less concerned with the costs of delivering IA. Academia certainly observes compliance objectives but I have no direct experience of how much effort and cost are applied to meeting IA objectives*
67S	*I suspect that the culture will only be adopted when a senior executive will pay the price for non-compliance.*
67S	*Getting caught is the crime. The effectiveness of audits to verify that information assets are protected appears highly suspect. In most cases bad press is the only impact with no penalties and no loss of job or employment rights.*

73S	*Academics are not providing enough good research (but that's because there is little funding available) and need to become more 'business-centric'*
76S	*Public sector have the 70 mandatory requirements from the SPF - whilst all sectors should take a risk based approach to IA, Government probably has the best articulated framework. A compromise would certainly be damaging in terms of PR, but ultimately the majority of Government departments are effective monopolies and their customers have little choice over whether or not to deal with them.*
76S	*Private Sector has fewer mandatory imperatives, but along with the third sector, potentially a far greater impact in terms of "customer perception" should they become compromised. Almost inevitably, it will lead to damaged revenue streams for these organisations.*
76S	*The academic sector is perhaps the most problematic. Traditionally, academia has focussed on sharing information and networks (such as JANET) are not renowned for their security features. Within academia, this is relatively well accepted through custom and practice, but can present substantial difficulties when academia attempt to work with the other sectors who are likely to seek evidence of how their information will be protected.*
77S	*Regulatory conformance is a priority but kite marks and certifications are being seen as superfluous*
45S **57S**	*Financial loss (lost revenue, fines, penalties, lawsuits, etc.), loss of business*
45S **57S** **73S**	*Loss of reputation / reputational damage –* *Maintaining reputation = measure of benefit and measurement overall*
46S **47S** **48S** **57S**	*Impact on brand / brand damage which could potentially be irrevocable*

Table 22: Drivers and Obligations - Coded Respondent Commentary

Standards and Measurements

Code	***Response commentary***
1F	*Better in terms of security may not be better in terms of efficiency*
10FS	*a. Through quicker/better achievement of the standards required by the MOD – IAMM Level 3 – and also a good way to ensure that the standard is maintained once achieved.* *b. Maturity needs followership just as important as leadership*
10FS	*IAMM dominates, but we are also interested in attainment of the ISO 27001*
10FS	*Managing issues – Head of IA Professions day job – undermining?*
15ES	*Confidence that we are protected*
48S	*Australian Federal Government InfoSec Management Framework* *Australian DoD – InfoSec Manual*
50S	*We have not identified compliance with any specific standard as a defined objective, and we don't measure the benefits of compliance. I would expect however that if we could demonstrate in an objective manner that we were in compliance with a relevant standard or set of standards, that this would provide benefits in terms of retaining my current account, competing for similar accounts, and as a potential legal defence in the event of a security incident by showing that we were diligent in following industry best practices.* (Note: this response was from the US healthcare sector, where HIPAA is the prevailing regulation, for which annual risk assessments are required – disappointing to see such a lack of situational awareness.*)*
50S	*We have no explicit programme of measuring the benefits. If asked to do so, I would approach it by quantifying the cost of InfoSec risks both before and after implementing security controls. Naturally, this would be time consuming (assuming a quantitative risk assessment had not previously been performed), and also highly subjective.*

54S	*Stringent regulatory controls and laws around the management of data have impacted all services both negatively and positively. Those laws, standards/policies and regulations are forcing the public and private sector to protect their assets better. I think that key public sector needs to probably look at better defences from a cyber warfare perspective and what strategic approach is needed in the next decade.*
56S	*When you process the IA you should be in a stable way of life with a minimum of threats, vulnerabilities and an identified risk potential and management. It's also a benefit to achieve with IA the best cost balance (risk management with the most cost-effective way) which is possible to reach and to reach finally best future financial calculations and plans.*
58S	*With the implementation of standard toolsets and monitoring software. For example, compliance testing software including vulnerability assessment software. Provision of high-level reports should be developed for management to understand the benefits provided by the IA group. What did we block, what could have been the impact, etc.*
62S	*Having to sell the idea to the Board makes this difficult*
71S	*Self-assessments (NHS, PCI)*
77S	*Risk mitigation criteria*
77S	*Regulatory compliance*
77S	*Benefits expressed in risk terms*
79S	*The Accreditor says "Yes".*
15ES, 52S	*Internal and external audit provide the measures*
31ES, 72S	*Qualitatively – effectively the absence of serious damage* *Cybersecurity cannot be measured as there are no cybersecurity standards – paralysing level of audit*

Table 23: Standards and Measurements - Coded Respondent Commentary

Impact of culture and politics

Code	***Response commentary***
1F	*State has responsibility*
7ES	***Security, data protection and privacy*** *– it was suggested that the DPA should support the development of clearer and more transparent definitions of the regulatory boundaries and limits which should apply to data collection and online tracking. This might for example include proposals for a more streamlined and intelligible list of options to help consumers explicitly consent for their personal data to be used in different ways (which are properly acknowledged and understood by the individual when this access is granted). The overarching objective should be to ensure that consumers are informed, protected and empowered, whilst ensuring that forthcoming regulations in this area do not constrain innovation, job creation or economic growth. ** (email comms 27 February 2011)*
7ES	*Yes. "Computer says no" and "Data Protection" are the new excuse for poor service. Compliance overheads combined with intrusive surveillance powers have led to high-value-added financial services moving key functions off-shore. You do not move to Switzerland to save money*
10FS	*Yes they do; it is important that the Government of the day plays due regard to the protection of information through its direct support and through its championship of other policies that might have an impact on the way information is used and protected*
10FS	*Need to survey to measure behaviour change*
14F	*When the eEnvoy was sponsor this was at Permanent Secretary level - Need an intelligent sponsor of HMRC to discuss*
15ES	*Large sections of the civil service do not operate in the fact driven environment that we have to inhabit in the commercial and related environments (e.g. professional, academic) - and we cannot force them to change, because they are a third but unaccountable power in the country: elected representatives, appointed government, civil service. Local Govt largely follows in the wake of the civil service [1]. So IA doesn't translate into many areas, but InfoSec does for those organisations that realise they must take the topic seriously as an extra component of ICT in their already well developed corporate governance strategy.*

15ES	*Creation, definition and mandation of standards required*
15ES	*Single most valuable thing*
15ES	*Seeking regulation*
15ES	*Systematic selling off of assets to shore up misguided spending, population of country exceeds capacity to support*
15ES	*No more assets to sell; more taxation required – or stop doing trident and HS2*
15ES	*Corporate world not applying integrity to its services*
15ES	*On the fault line; Erosion of corporate culture*
15ES	*** Previous public admin structures with their central policies, basic rules, and lots of freedom for the people out in the sticks to interpret policy and rules, allowed admin processes to adapt locally to local and even individual situations. The new centrally dictated processes, increasingly dependent on and monitored by IT systems (Still relatively low powered by today's standards) were poorly designed and unable to adapt to local needs, but the central teams simply became more and more isolated from reality and the quality of public admin started on a downward path. Classic civil service recruitment and career structures remained, but the private sector saw the need for new skills to be recognised at the highest level in an organisation, for the development of new methods of communicating with the front line and responding as necessary – and eventually with the need for formal quality management and then IT based InfoSec. Service delivery in the public sector was moving quickly from armies of people to computer processes – and the management failed to understand the need for quality engineering, for formal quality management, for very carefully targeted recruitment (to get the right people in the right jobs) and for continual staff development by way of training. … public sector failure to adapt results in situations where civil servants who want help are incapable of understanding what needs to be done. The many critical reports by Parliamentary Select Committees bear witness to the incompetence of so many Whitehall departments.*
15ES	*1997 to 2010 – no real opportunity to trigger change at central government level – the power of the mandarins (the third pillar of government, the others being parliament and the appointed executive) blocked any change and in many departments are still doing so.*
15ES	*….that Government sort of recognised the centrality of information and the need to control it when it set up the Government's DG of IM, along with the DG of Identity Management. The argument then, though, and still is that we need a central department to handle and protect Government Information and ensure its CIA rather than some DG with no real teeth. So is there a better way of "doing" IA than the UK is doing it now? Your answer is "Yes", because the current way is getting us nowhere. This of course needs a debate. Your great one pager sets this going but we probably need a workshop for you. Rather than re-organise IAAC, could I suggest your theme should be to re-organise Government? (email comms, 17 April 2011)*
15ES	*Get used to the feeling of déjà vu, is only another move through the cycle and in the end it still won't have changed. Pre-NPfIT and the poisoned dwarf in Leeds, there was a central security team with Regional Security Managers that interacted with the GPs, PCTs etc and progress had been made over a number of years. When NPFIT knifed the NHSIA in the back and retreated behind their websites so they didn't actually have to deal with people it all went to rats. Personally I did very well out of it all but security in the NHS went backwards and still hasn't recovered. NHS was well ahead of the curve in the late 1990s but died in 2005. The N3 Muppets put paid to it, because they didn't understand it and saw it as getting in the way and returned things to the anarchy it is today. The GSi CoCo was a direct lift from the NHSnet CoCo, I know, I saw them lift it. BTW it was always about budgets and how they managed them (email comms 25 April 2011).*
15ES	*I learned a while back that, under the gentle and capable hands of its former boss Richard Granger, that masterpiece of IT innovation called NPfIT (or 'Connecting for Health' as it subsequently preferred to describe itself) at one stage purchased, at a cost of £250 million, some 700 servers housed in several purpose-built data centres. Less than 6% of these servers were actually deployed or even had programmes installed. The mere support costs for that little lot was around £100 million per annum and the kit, after two years, was entirely scrapped for a 'refresh' at a cost of a further*

	£200 million. Total lolly squandered? Around £1.2 billion. It's this behaviour – both on the part of the Department of Health and the vendors concerned (they know who they are) – I find immoral and utterly lacking in integrity or competence. It hardly needs saying Government – especially Central Government – is particularly good at stuff like that (email comms 18 June 2010).
24T	*It's making the UK almost anti-competitive*
24T	*Not always focussing on the right things*
24T	*(Service sector culture); Operational security (horizontal) given up in favour of Security Services (vertical) – for the almighty dollar*
24T	*Politics is reactive – blame when an incident – a memory stick or a CD loss – but it is tangible result of a lack of security*
24T	*Public sector procurement is an issue*
24T	*Shared Services swathe 6 years ago – under Labour – but as a Policy – there were various software providers who acted as a tribe – IBM, Microsoft etc – said they would all be undermined – that it would be a national security threat*
24T	*Thus, the private sector is running the public sector ICT*
24T	*Outsourcing to big providers = fatal....*
24T	*Are the systems safe/are the right controls in the right place to maintain the safety?*
24T	*We have ended up with wrong systems architecture and this is leaving us with a legacy of problems.*
31ES	*There is more emphasis on IA these days but whether that is attributable only to the political landscape or whether it has been driven by the politics following some rather notable data losses by Government is difficult to assess. The cynic in me leans towards the later.*
31ES	*In the commercial sector there are some good examples but generally the feeling is that little has changed, and probably won't change until the ICO gets some high profile successes.*
35F	*One of the messages coming out from my meetings with Banks, Insurance and Law Firms has been the scale and nature of the culture gaps. The good news is that I have found a number of players looking to organise practical training on how to handle them - beginning with incident response - and the need to get InfoSec, forensics, compliance, legal counsel, marketing and PR working together while allowing IT to keep the business going ....*
35F	*Organisations don't think about security incidents – until they have one! Management attention quickly subsides after clean up. Evidence from series of risk assessment workshop demonstrates phenomenon of short-term corporate memory…Use this small window of opportunity to get what you want – pre-prepare projects, proposals, endorsements ready when window opens. Incidents are great opportunity to improve processes, controls, culture – I coined the phrase 'Surfing the Indignation" for increasing profile of InfoSec while management attention is still on the issue*
39FE	*Its people not just technology that needs patching*
39FE	*IA can be considered as a branch of Quality. Thorough application of the combined disciplines of QA and of engineering are essential throughout many of today's organisations, particularly in public administration: knowing what is to be done and carefully doing it. However, experience shows that many of the people involved in public administration are unable to think through the consequences of their designs.*
45S	*However, in those instances where security is a new operating paradigm for public sector entities, their response to security (particularly security incidents) has been known to be overzealous.*
46S	*It may be useful within my team if everyone has the same definition and understanding of the term. However, with customers, this is not really a well-known term so we tend to use a bunch of terms that covers IA like data, confidentiality, integrity, non-repudiation etc. as these are better understood by customers.*
47S	*… socio-political changes influenced by new media, applications and online services (Facebook etc). The younger generation is more connected and consumer driven, demanding more from employers and service providers. They vote with their 'likes' and 'dislikes'. Further, online political protests are taking on a new 'voice' with denial of service attacks seen as 'free speech' e.g. animal hactivists, political hactivists etc.*

48S	*Private Sector is more aligned to the 5 stages of grief: Denial, Anger, Bargaining, Depression (revenge), and Acceptance. I have seen this in a few companies, especially concerning PCI – the issue is one of the company being told to spend money on factors that are outside of their control (grief) and this requires taking leadership on the journey and trying to make the path as easy as possible.*
48S	*Wikileaks is driving a culture of fear in many Public Sector organisations but the influence of any political landscape is questionable. I see positive impacts in Australian Federal Public Sector in regards to IA but in State politics there is a level of self interest in political parties who do not want to see the evils of history make it into the light of day. In South Australia for example, the State Govt who have been in power for over 10 years have fought the introduction of an Independent Commission Against Corruption and are currently writing the legislation so that all ICAC investigations are totally confidential. This has not been driving a culture of accountability in the State Public Sector.*
48S	*SOC processes drive measurements*
49S	*Compliance with standards provide assurance to the customer that Information security is being carried out correctly and IT assets are being protected adequately.*
51S	*Wikileaks Incidents as well as loss or theft of F35 Fighter Aircraft Design as well as loss or theft of current US Nuclear Weapons Designs have highlighted the importance of this.*
52S	*Referencing the number of fines by the Information Commotion's [stet!] office towards the councils and government entities in recent years, it shows that IA is being taken seriously by the central government and in turn we are seeing a shift through the public sector.*
53S	*Identify and understand what has value to the considered business and the security it needs and where to allocate efforts and resources bridging the gaps between the actual state and the desired state*
53S	*The culture and behaviour is needed as well as awareness etc. appropriately is hard to define but regulation and compliance are tools for improving protection of information assets.*
56S	*Legal changes or regulations and political adoptions can provide and offer a new possibility of service sets/new UPSELL business as it was feasible before! With this in mind we should informed by legal or another alternative company instance when basics has changed and we can create more business profit and client benefit. This institution should teach sales and technical consulting personal as soon as possible!*
57S	*I have a few major government projects. They are very concerned about security and changing political landscape impacts their systems. That is why they have security clearance before one works on the project. The clearance is provided at a few categories depending on the nature of the information accessed and domain.*
57S	*The public sector client demands as many controls as many touch points to be implemented but the contractors may not be able to do so as their proposal did not factor in these costs. This results in stalemate and time is spent on interesting the intent of the contract and rounds of negotiation. Sometime it may end up in the solution deployment being delayed.*
62S	*Coalition government raised the priority of security in the cloud.*
69S	*Recent change of government, and their austerity measures, have all but killed-off public sector IA efforts with the bare minimum being undertaken.*
70S	*Yes :- 9/11 => increased risk awareness => increased risk understanding, awareness and management capability.*
71S	*Culture of care in the NHS, not a culture of security; it's changing but this will take time.... Public Sector and Private Sector – same issues, different scale(s)*
72S	*Positive changes in corporate governance in the private sector since the Cadbury Report*
76S	*Changes since the Hannigan Review have had a positive impact in public sector culture – primarily by raising awareness of the importance of IA.*
78S	*Currently yes its negative – Councils have to make significant cutbacks but we MUST ensure compliance to GCSx CoCo and it costs money (the Government haven't thought this through correctly)!*

80S	*Generally I would say the main driver for the public sector has been compliance and avoidance of bad publicity. The small culture change has been positive.*
7ES, 73S	*They have concentrated on ticking the boxes rather than protecting the assets. The growth of automated tools for generating and auditing procedures means that in some organisations no-one has read the processes, not even their nominal author, let alone understood them or their implications for operational efficiency, costs or "genuine" security*

Table 24: Impact of Culture and Politics - Coded Respondent Commentary

Professionalism of ICT and IA

Code	***Response commentary***
7ES	*The impact to date has probably been minimal. The BCS, for example, has made no real progress since it gained its Royal Charter and will not do so until its expels some-one for professional misconduct. I used to lecture on the previous code - with case studies and am back on the disciplinary panel. I know and respect the reasons for the lack of progress. No-one is willing to commit the funds to fight an appeal to courts by, for example, some-one working for a well-known consultancy on a well-known government project.*
10FS	*The public sector has become much clearer about the imperative to protect public and personal information. Industry has been surprisingly cooperative but some organisations might not have the resources to invest in the protective measures now expected of them.*
10FS	*Public sector awareness has risen very significantly, but behaviours are changing much more slowly than policies and processes. There remains much to do yet to get everyone to realise that forgetfulness and taking short cuts needs to be reduced.*
10FS	*There is a need too, to link the home to the work environment, to make the dangers of social networking to become more obvious and to provide much greater "built-in" security so that systems default to safe without irritating the user. Such changes would then make the difference between the public and private sectors to draw closer together.*
10FS	*I do not think professionalising IA or ICT has been the critical change. The most important change has been to move the use and protection of the information asset out of the technical sphere and to move it – both benefits and accountabilities – firmly into the centre of the business domain.*
10FS	*Need good trainers and deliverers and policy writers*
10FS	*Need to dispose of home hard drives*
10FS	*I would approach the IISP; I would take advice from the big 4 auditing firms, the insurance sector and high street banks; in extremis I would go to top ICT managed service providers for advice. I would probably do as well to go to successful public sector departments, such as Home Office, DWP and MOD.*
14F	*Outstanding project leadership skills and well developed concepts*
14F	*System of systems and human factors (HF) and ability to improve and lead*
14F	*Right people, right potential*
14F	*Need to come out competitive*
14F	*Still another five years away*
14F	*Prosecutions needed*
14F	*What are the components?*
14F	*What would good look like?*
14F	*Land, sea, air and information – new battle space – not attributed, fighting SMART*
14F	*Information superiority*
14F	*Should be able to run CIO government provided operational leadership are supportive*
14F	*SDSR / National Security Strategy / Cyber Security Strategy?*
14F	*Policy, strategy – coherent?*
14F	*Motion and no progress*
14F	*Need clearly stated objectives and milestones*
14F	*Operational costs will be swallowed*

14F	*Who do we engage moving forward?*
14F	*ECDL for Generation Z?*
14F	*Talent is key to the new reality – need to recruit and retain*
14F	*Part of delivering a good 21st century government*
14F	*Do not adjust your mind (set) there is a new reality*
14F	*Climate change?*
14F	*2008 crisis – fiscal etc*
14F	*Barriers to entry for adversary is low*
14F	*Issues – what are the needs and how can we align with these?*
14F	*Time constraints – no longer in a Cold War*
14F	*Academia to pay industry for their data?*
14F	*IA is only a post grad course really because it's too involved*
14F	*Need on the job experience etc*
14F	*Mix of social science, behavioural required*
14F	*Need people who challenge the status quo*
14F	*Frogs in boiling water – 1999 - mistakes about to be repeated?*
14F	*High turnover in Cabinet Office staff – not read SEB reports ☹*
14F	*How do you take your strategy forward in this fluid state? With a cadre of professionals….*
15ES	*(ISC)² has a common BoK that has been honed over 14 or so years. The IISP has a common BoK that has been put together over 3 or so years. SAN Institute is a good source of good practice and there are a number of Universities that offer post graduate degrees in the IA/IS space (Royal Holloway being one of the best known). If I were looking for an IA professional I would be looking for someone with a CISSP of good standing (i.e. someone who has maintained CPD and entered their second or subsequent 3 year phase of membership), someone who has membership of the IISP, someone who has held CLAS membership for three plus years or a person with an appropriate MSc. Preferably I would be looking for a combination of two or more of these attributes*
17E	*Information security awareness is seriously miss-named in a way that inhibits proper selection of controls over the vulnerable human element. Everybody hates security. It gets in the way of work performance; it's a bother concerned with incidents that rarely happen; and being aware of security just assists people to take a chance and violate the security controls that they don't like or even assists them in engaging in cybercrime. Hinson makes this clear in two of his quotes:* *"No one wants security…" Steve Hunt* *Mich Kabay: "…resisting the herd's anti-security bias."* *We should be creating InfoSec motivation, not just awareness, training, or education. Motivation is what counts. Calling it awareness deceives and misdirects management. Awareness, training, and education are worse than useless without first creating the motivation to support security that people don't like. Hinson makes this clear by including the following quotes:* • *ISF Standard of Good Practice and the DTI Factsheet: "…linking security to personal performance objectives/appraisals." (taken from my early writings)* • *Mich Kabay writes about creating commitment to InfoSec* • *The NIST Special Publication 500-50 mentions motivation.* • *The Noticeboard advises, "Enforce the rules."* *We must become very specific on this requirement because the human resources departments in many organisations resist the motivation controls that we must have. The controls are quite obvious when you consider what it takes to motivate employees and other stakeholders to engage in practices they don't like. I have been recommending this in my consulting practice for 45 years. The control objective is to make and enforce security as part of job performance and not be in conflict with it. We do this in three ways:* 1. *Include the requirement for InfoSec in all personnel and contract job descriptions and enforce it top to bottom in the hierarchy.* 2. *Include security as an evaluation subject item in all annual personnel and contract job performance and appraisal reviews*

	3. *Establish and uniformly apply fair and meaningful rewards for exemplary security and penalties for poor and failed security* *Here is one final note on Hinson's otherwise excellent article. Hinson writes about needing to protect the confidentiality, integrity, and availability (CIA) of information. You may have heard me expound on this many times, but it is worth repeating because of its basic nature. I might conclude (but don't because he is just being usage-correct) that he believes:* • *We don't have to be concerned about protecting the possession of proprietary but not necessarily confidential information such as from commercial software piracy.* • *We don't have to protect against modification of information that doesn't affect its integrity (dictionary: good condition) such as in cyber-fraud.* • *And we don't have to care whether information is useful as long as it is availability such as encrypted information where only the key is unavailable; the information still available, but just not useful in its present form.* *I'm sure he doesn't believe this stuff, but CIA doesn't cover it. I continue to point out that the excessive simplification of security factors by restricting InfoSec to protecting CIA is short-sighted and dangerous.*
20F	*It could be that professionalising IA is in error because it risks the journey to IG.*
20F	*Heads of Profession – not IA professionals – perpetuating unprofessionalism….*
20F	*Research on professional bodies – IET, IIA, ICA, IOD, IPD – is there consistency in the skills sited?*
31ES	*Within central government there is now focus on the supply chain though from speaking to fellow practitioners, this focus is somewhat fragmented. My experience however is that the supply chain is involved and to a high degree.*
31ES	*IA and InfoSec is a maturing profession and can only serve to enhance the role of IA/IS within an organisation. There is a lot of good practice with Government as exampled by the CESG CLAS scheme (CLAS = CESG Listed Advisor Scheme) which for a number of years has undertaken to create a body of IA professionals. Even this scheme has undergone a number of changes over recent time as the level of professionalism has increased. However there has been little transference of this expertise to into the private sector. However the existence of* (ISC)² *and its CISSP qualification, the emergence of the IISP coupled with a renewed drive on the security and risk front from within the BCS will help drive better practices into the commercial arena.*
39FE	*IG should exist outside IT within a corporate governance structure. Security technology IS IT, but it is just IT. Financial and other process Audit is not part of IT so why should security sit within IT. The effect of that model is that they are both poacher and gamekeeper and that cannot be right. Because of the changing characteristic of data security and its increasing legal obligation, existing within a legal structure I wouldn't resist. Need to align with LEGAL.*
57S	*This is a sensitive question. My experience and exposure is as follows :* • *Client is concerned about security and wants the best* • *Contractor personnel unable to give the consideration and emphasis to security. Many not aware of hardening requirements, secure coding principles and some not aware of the ISMS policy* • *Touch points instituted for personnel to comply with Security. The challenge is that they are doing it because they are being told and not that it will help to make a better product/outcome. They see security as an obstacle and will bypass if given the choice.* • *My personal view is that top management should walk the talk e.g. by walking around the office area or spreading/enforcing the mantra in town hall meetings* • *CISO tenure less than five years and turnover running at 20% per annum – fired at twice the rate of any other professional (16 months as of Sept 2015)*
57S	*On the positive side, professionalising the industry serves to enhance better standards in terms of knowledge and methodology. However, on the negative side, InfoSec changes are rapid and this may impede the speed at which IT security is able to evolve to meet new demands / requirements.*

57S	*If he is new entrant to InfoSec would suggest SANS Security Essentials (GSEC). I attend this course in 2000. The concept of Triad of Security (C, I, A) was introduced. Over the last 13 years, my understanding of the concepts has deepened tremendously and interaction/engagement with the clients has been positive and professional. Every issue can be analysed and presented with the attending facts (Risk Assessment) and recommendations.*
47S	*My experience is there has been attempts to improve InfoSec (IA to a lesser degree) in the public sector (state Vic and federal Aust) however this has wavered during the GFC. There has been significant loss of resources (employees and contractors) in the public sector and significant cost cutting, resulting and a negative impact on IA/InfoSec. The public sector makes gradual advances as technology and the individuals in general improve in education and awareness, training, resulting in the protection of information assets.*
48S	*I like the idea of professionalising the industry as it has given business leaders a better term of reference to gauge the capabilities of individuals in recruiting but also has allowed for people to move further up the leadership ranks as the training allows for a much better alignment of IA to business strategy adding more value and influence to the organisation in IA.*
48S	*I had a case of the Senior Leader for risk compliance had every professional certification under the sun but he had no experience and I had to train him in his role.*
49S	*Various certification bodies provide lists of certified professionals.*
50S	*I believe that security tends to be perceived in many organisations as either a highly technical discipline or as an administrative issue, but not as an area of management focus (comparable with finance, for example). At my account, even though the ASO is shown on client-facing organisation charts as reporting directly to the Account Executive (and therefore part of the management team), in practice I report to a second-level manager and am excluded from management meetings. This has a negative impact on my ability to encourage change at an account which for many years has not followed many basic security practices.*
51S	*Emphasis on ICT technology has had a negative impact on IA by providing a false sense of security (Good AV, Patching, Firewalls, IPS, Access Control are necessary but not sufficient to protect confidential information).*
52S	*There is a steady slow progress as when comparing to the past decade, IA positions were unheard of and now they are part of the DNA of any prominent organisation. There is a paradigm shift from compartmentalized ITSec functions with point based technical security solutions to hybrid federated IA functions focusing enterprise risk management as a whole. Requirements of IA within roles and organisational structures are yet to be seen.*
52S	*Senior peers, ISACA, local shapers, thought leaders, blogs, webinars, webcasts, conventions, trainings, specialised magazines…etc.*
53S	*Experience is an important key combined with leadership and tech knowledge*
56S	*I try to explain it this way: I believe that everyone is informed in a let's say common syntax and understanding of the industry requirements and so it is a platform we can use for optimal communication between all relevant parties.*
56S	*It helps to let folks understand what we do, how we do it and why we do following these standards and requirements.*
56S	*Also a lot of reports in the industry are standardized more or less this way. It allows us to work with a lot of specialized teams on all these items, means we are more effective, quicker and more precise when following these standards, helping us DON'T forget any of these important aspects.*
59S	*With cyber-attacks steadily increasing, the majority of the culture realizes the importance of effectively securing their assets and their clients. However, they continually face budget constraints and therefore must find more cost effective measures.*
61S	*Improvement progress is visible but the pace is frustrating*
65S	*I do not believe the term IA is helpful to people who do not have a background in either secure systems or IA.*

67S	*In the public sector there is more of an awareness that the info may be sensitive and they are not the 'owner' of that info...still a long way to go before individuals in their day-to-day operations consider IA appropriately. Specialists in the field are aware but it needs to be wider and higher in the organisation.*
69S	*Professionalisation is (IMHO) yet to be completed with the relevant organisations (BCS/IISP) dealing with internal matters too much and failing to sell the benefits to IA consumers.*
69S	*Crystal ball - Public sector is expecting supply chain to be practice IA but contractual terms are woefully inadequate and not being policed – further breaches are inevitable.*
71S	*Continued failures of IT projects, such as the recently abandoned Identity Access Management system for NHS Scotland, does not paint a picture of the industry as one which can deliver any benefit. Under these terms it is no surprise IT is one of the first casualties when it comes to cost saving since 'they always waste the money they are given don't they?'*
72S	*Cadbury Report improved Corporate Governance*
76S	*I have seen little evidence of impact. Competent individuals remain competent. The professionalisation of ICT has had little impact on recruitment practices, and hence there are still "less competent" individuals employed.*
77S	*This has had an overall negative effect as IA activities are moved out of main stream activities*
78S	*…but there are a lot of staff that have not had any real training let alone get certified in anything (if they did, they would almost certainly leave to a better paid job).*
79S	*They tend to over react. Also larger divergences in approach and what is "acceptable" security.*
79S	*Check all sources. No single source stands out at the moment.*
80S	*The competency of an organisation is based on the people it employs. If minimum standards are required, such as professional certification (e.g. from ISACA and (ISC)², are starting to become standard requirements for ICT/IA roles this has a positive impact as it weeds out the real duffers.*
80S	*ISACA and* **(ISC)²** *are the only organisations with a reliable minimum level of competence required from their members in this area.*
10FS, 77S	*Reduced – opposite to above*
46S, 60S, 74S	*Positive impact; but more mandatory processes should be considered when awarding Govt contracts. Important that they are mutually agreed, and not too bureaucratic. It's the CIO and CTO that need to understand this – not just the CISO, also the CIRO, and the CRO – we have too many roles and verticals.*
46S, 63S, 75S	*Manufacturing lags behind* *Can't aim for perfection but have to build in change gates*

Table 25: Professionalism of ICT and IA - Coded Respondent Commentary

InfoSoc

Code	***Response commentary***
24T	*We are not creating homogenous foolproof easy to use, low cost computing*
24T	*Safety = people die; Security = ??*
34F	*Decision making is currently too slow – because we are not communicating*
34F	*As low as reasonably practical*
35F	*My own opinion - there shouldn't be a "security market" at all - the skills, experience, knowledge and "ways of working" need to be embedded in every other industry, and then we can all retire. Things are heading that way, thankfully.*
35F	*Lack of understanding in the market = lack of appreciation of true value of information assets in the market place*
41E	*Riding the dragon's tail – GRC – in that order for a reason! Not a fun ride if you go the wrong way around.*

Table 26: InfoSoc - Coded Respondent Commentary

Barriers

Code	*Response commentary*
14F (on behalf of IAAC)	***Insufficient action by governments*** • *E Government wired up by 2005; gone off the boil.* • *eCrime strategy: good ideas, yet to be seen, make sure momentum keeps up!* • *Computer Misuse Act: over 10 years old (except for one minor review in 1999!) long overdue overhaul.* • *RIPA (Regulation of Investigative Powers Act): poor legislation, introduced too swiftly, already subject to change.* • *Data Protection Act: well-founded sentiments, but poorly executed causing immense confusion (Soham murder trial)* • *National and international cooperation at the working level works well between police forces (National High Tech Crime Unit)* • *Grand Bargain between privacy and functionality* • *Intelligence, security and resilience – Paddy McGuinness* • *Expectations of service and dependencies*
	Insufficient awareness by citizen • *No coherent view on citizens' role and responsibilities and liabilities yet* • *Education and behavioural norms by osmosis* • *When aware, the means to act responsible are not easily available*
	Insufficient coherence of action by industry • *Still not a board issue.* • *Information exchange on attacks and vulnerabilities still difficult* • *Benchmarking is promising, but industry waits for the first to engage in it (first adaptors are waited for)* • *Protecting yourself is not (yet) been made easy with complementing technologies and services from multiple providers* • *Getting better, due to efforts of trusted bodies and trade bodies*

Table 27: Barriers - Coded Respondent Commentary

Observations:

Risk management profession needs to welcome the assurance that the other IA provide that the controls they rely on are working effectively as intended (Marks, 2015, p.192).

Goldman Sachs expose – 14 March 2012, Evening Standard – "Today if you make enough money for the firm (and are not an axe murderer) you will be promoted." Attitude / not putting the customer first….

When asked to provide a good book or resource for a new Security Officer, the following were the suggestions (three of which appear in the Bibliography in full Harvard format):

- *"Adaptive Security Management Architecture" by James S. Tiller*
- *The Company InfoSec Policy*
- *Something by Kevin Mitnick*
- *"Security in Computing" by Charles and Shari Pfleeger (for those with strong technical backgrounds)* ***or*** *NIST 800-100; InfoSec Handbook: A Guide for Managers (for those with non-technical backgrounds).*
- *CISSP All-in-One Exam Guide, 6th Edition. Shon Harris. Note that although this is a study guide for the CISSP exam, it is also a well-written and frequently updated survey of security topics of interest to security practitioners.*
- *"How to cheat at Managing InfoSec" by Mark Osborne*
- *"Secrets and Lies: Digital Security in a Networked World" by Bruce Schneier*
- ***"****Cyber War: The Next Threat to National Security and What to Do About It" by Richard A Clarke*
- *"The $100 Start-up" by Chris Guillebeau*

10.18 IA Search Methodology and Other Information Sources for IA

10.18.1 The research timeline can be described as follows:

- **2009-2010** IA literature: methods, technologies and management frameworks
- **2010-2011** IA literature: chronological historical development (continually revisited and updated)
- **2011-2014** IG / GRC / ethnographic research in action
- **2014-2016** Organisational structure, problem structuring and solving, mixed methodologies, reflexivity, Grounded Theory formulation and framework development.

10.18.2 Several libraries, search engines and available databases were searched for publications information dealing with IA (last checked 7 September 2016):

- University of Wolverhampton library resources - wlv.ac.uk/lib
- COPAC - copac.ac.uk/
- The British Library - bl.uk/
- INTUTE - intute.ac.uk/
- World Catalogue – worldcat.org/
- DOAJ – www.doaj.org/
- OAISTER - oaister.worldcat.org/
- ETHOS – ethos.bl.uk/
- Google Scholar – scholar.google.co.uk/
- Google – www.google.co.uk and www.google.com and https://sites.google.com/a/aubih.edu.ba/cita-250/references

10.18.3 Other sources utilised were:

- *Books*
- *Government Reports*
- *Official documents*
- *Academic publications*
- *Industry Publications / Reports*
- *Vendor Reports*
- *Industry Journals, including IS Journal (ISJ)*
- *Online Sources – blogs, articles etc*
- *Trade Body Reports*
- *Membership Body Reports*
- *Documents*
- *Interviews*
- *Direct observations*
- *Participant-observation situation*
- *IAAC library - http://www.iaac.org.uk/library-resources/library/*

10.18.4 **Note**: the researcher was responsible for the creation of a great many of the Briefing Papers available in the historical library repository of IAAC.

10.18.5 Table 28 represents the collation of the volume of IA work identified:

Academic Journals	Ashley, B., Cox, S., Dean, T. and Stimeare, R. (1999) Bannister, F. (2002) Cherdantseva, Y. and Hilton, J. (2013a) D'Aubeterre, F., Singh, R. and Iyer, L. (2008) Dark, M.J., Ekstrom, J.J. and Lunt, B.M. (2006) Endicoytt-Popuvsky, B. (2003) Ezingeard, J.-N., McFadzean, E. and Birchall, D. (2007) Gericke, A., Fill, H. G., Karagiannis, D. and Winter, R. (2009) Hamre, J. (1998) Ilies, I.M. and Boaru, G. (2011) Liles, S. and Kamali, R. (2006) Powell, R., Holmes, T.K. and Pie, C.E. (2010) Stahl, B.C. (2004) Valeri, L. (2001)
Conferences and Panel Discussions	Abdullah, N., Sadiq, S. and Indulska, M. (2011) Cherdantseva, Y. and Hilton, J. (2013b) Flechais, I., Riegelsberger, J. and Sasse, A. M. (2005) Gillon, K., Branz, L., Culnan, M., Dhillon, G., Hodgkinson, R. and MacWillson, A. (2011) Maconachy, V., Schou, C., Ragsdale, D. and Welch, D. (2001) McCumber, J. (1991) Piatek, M. and Newkirk, J. (2009) Saltzer, J. and Schroeder, M. (1975) Shanes, P. and Ciechanowicz C. (2011)
Empirical Research	Beauregard , J.E. (2001) Burnburg, M.K. (2003) Bush, S. and Evans, S. (2001) Cherdantseva, Y. and Hilton, J. (2013) Cherdantseva, Y. (2014) Coles-Kemp, E. (2008) Cornish, P., Livingstone, D., Clemente, D. and Yorke, C. (2011) Dimopoulos, V.A (2007) Fox, J.M. (2003) Fenz, S., Goluch, G., Ekelhart, A., Riedl, B. and Weippl, E. (2007) McFadzean, E., (2005) Weill, P. and Ross, J. (2005) Nanton, T.J. (2004) Pappas, J.A. (2008) Racz, N., Weippl, E. and Seufert, A. (2010) Simmons, A. (2016) Spafford (2001) Vaidya, T. (2015) Valentine, E. (2015) Vicente, P.F.O. (2011)
Books	Blyth, A.J.C. and Kovacich, G.L. (2001 and 2006) Desman, M.B. (2002) Herold, R. and Rogers, M.K. (2010) Herrmann, D.S. (2002) Peltier, T.R. (2001, 2002, 2004, 2005) Schou, C. D. and Trimmer, K. J. (2004) Schou, C. and Shoemaker, D. (2007)

Table 28: Special Issues, Conferences and Studies in IA Research Relevance

10.18.6 The following resources are provided as evidence of the breadth of availability of best practice guidance.

General IA Search Resources:

[Last Accessed 12 September 2016]. Available at: http://www.answers.com/topic/information-assurance-2

Norman Marks – blogs, articles etc. Available at: http://normanmarks.wordpress.com/2011/02/15/protiviti-provides-sound-insights-into-risk-management-failures/

Industry Journals monthly publications and online resources:

Government Computing – *Government Computing* Magazine, monthly, www.kable.co.uk, moved to www.guardian.co.uk/government-computing-network

Cryptogram – monthly newsletter by Bruce Schneier - https://www.schneier.com/crypto-gram/

Corporate Compliance Insights - https://www.google.com/webhp?sourceid=chrome-instant&ion=1&espv=2&ie=UTF-8#q=corporate%20compliance%20insights%20james%20bone

Data Loss information, www.datalossdb.org

IISP - Institute of InfoSec Professionals – Pulse magazine, https://www.iisp.org/imis15/

ISACA Journals 2000 through to 2017, Illinois: ISACA, www.isaca.org

(ISC)² *InfoSecurity Professional* magazine, www.isc2.org

ISM - InfoSec Magazine (ongoing), http://searchsecurity.techtarget.com/

ISSA Journals 2000 through to 2017, Oregon: IS Security Association

IWAR, *Information Warfare*, http://www.iwar.org.uk/iwar/

Krebbs on Security – blog - https://krebsonsecurity.com/

TheGRCBlueBook.com - http://thegrcbluebook.com/

The Industrial Control Systems Cyber Emergency Response Team (**ICS-CERT**) - https://ics-cert.us-cert.gov/

10.18.7 The researcher was involved in the UK Government Fore*sight* Cyber Trust and Crime Prevention (CT&CP) Project in the Autumn of 2003. The project produced the following related outputs:

- Full papers
  - **Social Risk Management – Practices and Behaviour in Cyberspace** Dr James Backhouse, LSE
  - **Social Learning and Trust in Cyberspace: Issues of Reciprocity** Professor William Dutton, OII, Oxford University
  - **Usability Issues and Trust in Cyberspace**
  - **Knowledge Technologies**: Professor Nigel Shadbolt, Southampton University
  - **Identification and Authentication**: Professor Fred Piper, Royal Holloway
  - **Autonomous Agent Technologies**: Professor Nick Jennings, Southampton U.
  - **Dependability and Trustworthiness**: Professor Cliff Jones, DIRC, Newcastle U.

- Short papers
  - ↘ **Crime and Crime Prevention**: Professor Ken Pease, Huddersfield University
  - ↘ **The Economics of Trust in Cyberspace:** Jonathon Cave
  - ↘ **Legislative and Regulatory Issues in Cybercrime Prevention:** John Edwards
  - ↘ **Civil Liberties in Cyberspace**: Gus Hosein, LSE

10.18.8 The project context and subjects raised are shown in Figure 87 below:

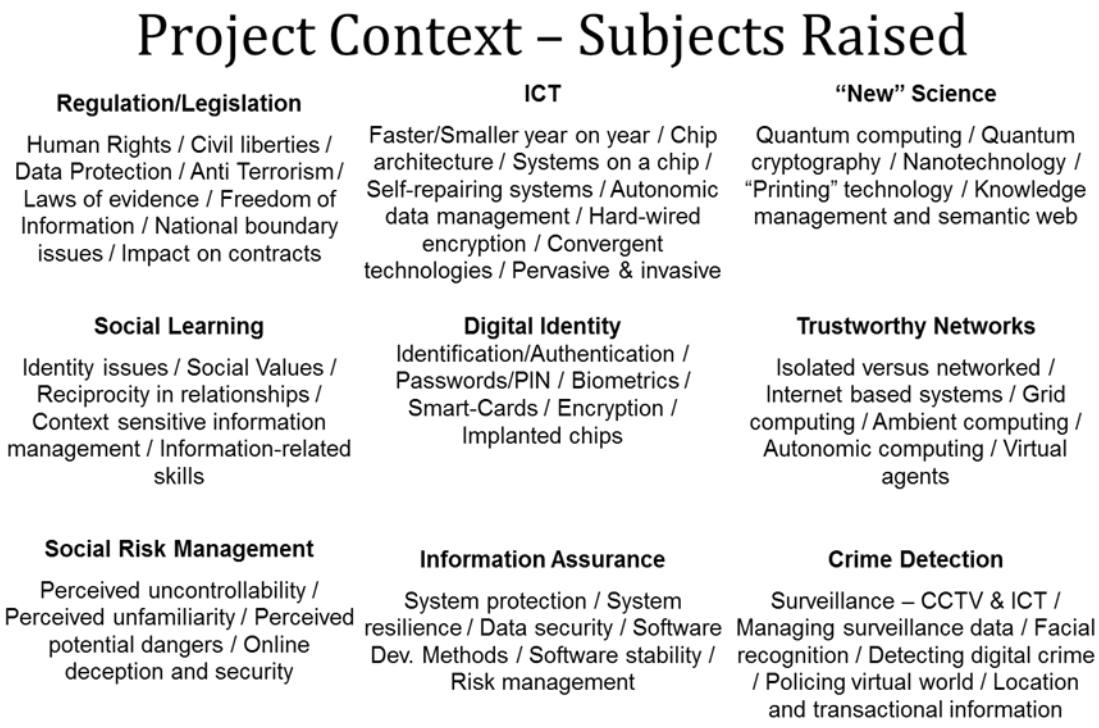


Figure 87: CT&CP Project Context - Subjects Raised, Source: UK HMG (2003a)

10.19 Available Related Standards and Best Practice Resources

Standards - listed in Standard number order, in the case of BSI

American Institute of Certified Public Accountants, Inc (AICPA) and Canadian Institute of Chartered Accountants (CICA) (2006) Trust Services (SysTrust) Principles and Criteria for Systems Reliability – addresses Availability, Security, Integrity, Maintainability - http://www.webtrust.org/download/Trust_Services_PC_10_2006.pdf

Australian Government Defence Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions - http://www.asd.gov.au/infosec/mitigationstrategies.htm

Basel Committee on Banking Supervision (2013) Principles for effective risk data aggregation and risk reporting, BCBS239 - http://www.bis.org/publ/bcbs239.pdf This will change the dynamic of breach reporting. From 2017 responsibility to report is within a week; from 2019 the requirement is to report within 15 mins.

British Standards Institution (2003) BIP 0002 Guidelines for the use of personal data in system testing, Jenny Gordon and Louise Wiseman *– Egg plc, September 2003, London: BSI*

British Standards Institution (2008) BIP 0008-1 Evidential Weight and Legal Admissibility of Information Stored Electronically. Code of Practice for the Implementation of BS 10008, London: BSI.

British Standards Institution (2008) BIP 0008-2 Evidential Weight and Legal Admissibility of Information Transferred Electronically. Code of Practice for the Implementation of BS 10008, London: BSI.

British Standards Institution (2008) BIP 0008-3 Evidential Weight and Legal Admissibility of Linking Electronic Identity to Documents. Code of Practice for the Implementation of BS 10008, London: BSI.

British Standards Institution (2001) PD 6668: 2001 *Managing Risk for Corporate Governance, London: BSI*

British Standards Institution (2006) BS 7858:2006 Security screening of individuals employed in a security environment – Code of practice, London: BSI. BS 7858 is a key security standard that tells you how to screen staff before you employ them. BS 7858 gives recommendations for the security screening of individuals to be employed in an environment where the security and safety of people, goods or property is of extreme importance. It also applies when there is a requirement of the employing organisation's operations and/or where such security screening is in the public interest. + Amendment 2:2009

British Standards Institution (2001b) The TickIT Guide: Using ISO 9001:2000 for Software Quality Management System Construction, Certification and Continual Improvement, London: BSI

British Standards Institution (2004) ISO 13335:2004 Information technology -- Guidelines for the management of IT Security, London: BSI.

British Standards Institution (2012) BS ISO 14721:2012 Space data and information transfer systems. Open archival information system (OAIS). Reference Model, London: BSI. A reference model for what is required for an archive to provide long-term preservation of digital information.

British Standards Institution (1998), BS ISO/IEC TR 15846 Information technology. Software life cycle processes. Configuration management, *London: BSI*

British Standards Institution (2012) BS ISO 16363:2012 Space data and information transfer systems. Audit and certification of trustworthy digital repositories. London: BSI. Sets out comprehensive metrics for what an archive must do, based on OAIS. Known as the Magenta Book or the Pink Book, September 2011

British Standards Institution (2014) BS ISO 16919:2014 Space data and information transfer systems. Requirements for bodies providing audit and certification of candidate trustworthy digital repositories. London: BSI. Specifies the competencies and requirements on auditing bodies.

British Standards Institution (2000) ISO/IEC 17799 (BS 7799) *Part 1:2000 Information security management: Code of practice for InfoSec management*, *London: BSI*

British Standards Institution (2004) ISO/IEC TR 18044:2004 Information technology -- Security techniques -- Information security incident management, London: BSI.

British Standards Institution (2002) ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing, London: BSI

British Standards Institution (2011) ISO/IEC 20000-1:2011 Information Technology Service Management, Part 1 Specification, London: BSI.

British Standards Institution (2011) ISO/IEC 20000-2:2011 Information Technology Service Management, Part 2 Code of Practice, London: BSI.

British Standards Institution (2012) ISO/IEC 22301:2012 Societal security – Business continuity management systems – Requirements, London: BSI. ISO 22301 standard has replaced BS 25999-2, and is considered the fundamental business continuity standard because it defines the basics of developing and managing the BCMS; this is the only certifiable business continuity standard. It is useful in the Do Phase according to ISO 27001 for the implementation of requirements given in its Annex A Chapter 14 (business continuity management).

British Standards Institution (2012) ISO/IEC 22313:2012 Societal security – Business continuity management systems – Guidance, London: BSI.

British Standards Institution (2015) ISO/TS 22317:2015 Societal security – Business continuity management systems – Guidelines for business impact analysis (BIA), London: BSI. Shows BIA paired with Risk Assessment, in keeping with ISO22301.

British Standards Institution (2015) ISO/TS 22318:2015 Societal security – Business continuity management systems – Guidelines for supply chain continuity, London: BSI.

British Standards Institution (2013) ISO/IEC 24762:2008 Information technology — Security techniques — Guidelines for information and communications technology disaster recovery services, London: BSI. This is the international standard that offers guidelines on the provision of ICT disaster recovery (ICT DR) services as part of business continuity management (BCM).

British Standards Institution (2008) BS 25777:2008, *Information and communications technology continuity management, Code of practice, London: BSI*

British Standards Institution (2006) BS 25999-1:2006 Business continuity management – Part 1: Code of Practice, London: BSI. BS 25999-1 gives guidelines for the implementation of each business continuity element.

British Standards Institution (2007) BS 25999-2:2007 *Business continuity management – Part 2: Specification, London: BSI*

British Standards Institution (2013) ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements, London: BSI. - The ISO 27001 Standard is the fundamental InfoSec management standard because it defines the basics of "building" and controlling an ISMS; this is the only certifiable InfoSec management standard, worldwide. See http://www.iso27001security.com/html/27001.html *and* http://advisera.com/27001academy/knowledgebase/information-security-business-continuity-standards/

British Standards Institution (2013) ISO/IEC 27002:2013 Information technology - Security techniques - Code of practice for InfoSec controls, London: BSI - ISO/IEC 27002 (formerly ISO/IEC 17799). This standard gives a more detailed description of implementation of controls, and is mostly applied in the Do Phase (Implementation) of ISO 27001.

British Standards Institution (2010) ISO/IEC 27003:2010 Information technology — Security techniques — Information security management system implementation guidance — Requirements, London: BSI. This Standard focuses on the critical aspects needed for successful design and implementation of an InfoSec Management System (ISMS) in accordance with ISO/IEC 27001:2005.

British Standards Institution (2009) ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement, London: BSI. This standard provides guidance on the development and use of measures and measurement in order to assess the effectiveness of an implemented InfoSec management system (ISMS) and controls or groups of controls, as specified in ISO/IEC 27001.

British Standards Institution (2011) ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management — Measurement, London: BSI. This standard specifies methods for information risk assessment and treatment, and is useful in the Plan Phase according to ISO 27001.

British Standards Institution (2011) ISO/IEC TR 27008:2011 Information technology — Security techniques — Guidelines for auditors on InfoSec controls — Measurement, London: BSI. This standard provides guidance on reviewing the implementation and operation of controls, including technical compliance checking of information system controls, in compliance with an organisation's established InfoSec standards.

British Standards Institution (2013) ISO/IEC 27014:2013 Information technology — Security techniques — Governance of InfoSec, London: BSI.

British Standards Institution (2011) ISO/IEC 27031:2011 Information technology — Security techniques — Guidelines for information and communications technology readiness for business continuity, London: BSI. This standard has replaced BS25777 and describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects for improving an organisation's ICT readiness to ensure business continuity

British Standards Institution (2011) ISO/IEC 27034-1:2011 Information technology — Security techniques — Application security – Part 1: Overview and concepts, London: BSI.

British Standards Institution (2015) ISO/IEC 27034-2:2015 Information technology — Security techniques — Application security – Part 2: Organisation normative framework, London: BSI.

British Standards Institution (c.2017) ISO/IEC CD 27034-3 Information technology — Security techniques — Application security – Part 3: Application security management process, London: BSI. [conversion of OWASP]

*British Standards Institution (planned) ISO/IEC CD 27034-4 Information technology — Security techniques — Application security – Part 4: Application security validation, London: BSI. [*cancelled*]*

British Standards Institution (planned) ISO/IEC CD 27034-5 Information technology — Security techniques — Application security – Part 5: Application security – Protocols and application control data structure, London: BSI. [draft]

British Standards Institution (planned) ISO/IEC CD 27034-6 Information technology — Security techniques — Application security – Part 6: Case studies, London: BSI. [draft]

British Standards Institution (planned) ISO/IEC CD 27034-7 Information technology — Security techniques — Application security – Part 7: Application security assurance prediction, London: BSI. [draft]

British Standards Institution (2011) ISO/IEC 27035:2011 Information technology — Security techniques — Information security incident management, London: BSI.

British Standards Institution (2014) ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships – Part 1: Overview and concepts, London: BSI.

British Standards Institution (2014) ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships – Part 2: Requirements, London: BSI.

British Standards Institution (2013) ISO/IEC 27036-3:2013 Information technology — Security techniques — Information security for supplier relationships – Part 3: Guidelines for information and communication technology supply chain security, London: BSI.

British Standards Institution (2014) ISO/IEC 27036-4:2014 Information technology — Security techniques — Information security for supplier relationships – Part 4: Guidelines for security of cloud services, London: BSI.

British Standards Institution (2011) BS ISO 30300:2011 Information and documentation — management systems for records. Fundamentals and vocabulary, London: BSI. This standard explains the purpose of a Management System for Records (MSR), the principles for successful implementation and provides the terminology for using MSR standards, compatible with other management systems standards.

British Standards Institution (2011) BS ISO 30301:2011 Information and documentation — management systems for records. Requirements, London: BSI. This is the specification of requirements for developing records management policy, objectives and targets to implement organisation-wide improvements. This is done through defining roles and responsibilities, designing processes and systems, allocating appropriate resources and measuring and evaluating outcomes, to ensure corrective action is taken and continuous improvement occurs.

British Standards Institution (2009) BS ISO/IEC 31000:2009 Risk Management. Principles and guidelines, London: BSI. ISO 31000 provides high level principles and generic guidelines for Risk Management.

British Standards Institution (2009) ISO/IEC 31010:2009, *Risk management – Risk assessment techniques*, *London: BSI*

British Standards Institution (2008) BS ISO/IEC 38500:2008 Corporate governance of information technology, London: BSI. This standard provides guiding principles for directors of organisations on the effective, efficient, and acceptable use of Information Technology (IT) within their organisations. It applies to the governance of management processes (and decisions) relating to the information and communication services used by an organisation. These processes could be controlled by IT specialists within the organisation or external service providers, or by business units within the organisation. This standard shows governance and management as critical to addressing business pressures and business needs.

British Standards Institution (2013) PAS 555:2013 Cyber security risk. Governance and management. Specification, London: BSI. Offers an outcome-based approach to Cyber Security.

British Standards Institution (2014) PAS 754:2014 Software Trustworthiness. Governance and management. Specification, London: BSI.

British Standards Institution (2010) PD 25111:2010 Business continuity management. Guidance on human aspects of business continuity, London: BSI. This standard gives guidance on the planning and development of human resource strategies and policies for the key phases following a disruption: Coping with the immediate effects of the incident, Managing people during the period of disruption (the continuity stage), and Supporting staff after recovery of normal operations.

British Standards Institution (2010) PD 25666:2010 Business continuity management. Guidance on exercising and testing for continuity and contingency programmes, London: BSI. This gives appropriate guidance on performing exercising, including testing activities, for continuity and contingency programmes. Arrangements for information technology (IT) systems also fall under this general guidance.

Building Security In Maturity Model Software Security Framework (BSSIM SSF) https://www.bsimm.com/online/

Capability Maturity Model (CMM) http://cmmiinstitute.com/

CERT – OCTAVE method is an approach used to assess an organisation's InfoSec needs. http://www.cert.org/resilience/products-services/octave/

COSO, http://www.coso.org – The Committee of Sponsoring Organizations of the Treadway Commission (COSO) is a joint initiative of the five private sector organizations – AAA, AICPA, FEI, IMA and the IIA develops frameworks and guidance on enterprise risk management (ERM), internal control and fraud deterrence.

CRAMM (CCTA Risk Analysis and Management Method) - https://managementmania.com/en/cramm-ccta-risk-analysis-and-management-method See also: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

EA 7/03 (1997) EA exists to coordinate and lead the European accreditation infrastructure to allow the results of conformity assessment services in one country to be accepted by Regulators and the market place in another country without further examination, for the benefit of the European community and the global economy. http://www.european-accreditation.org

European Banking Authority (2014) Guidelines on internet payments security - https://www.eba.europa.eu/regulation-and-policy/consumer-protection-and-financial-innovation/guidelines-on-the-security-of-internet-payments

ENISA - listed all the documents of National Cyber Security Strategies in the EU but also in the world (latest update April 2013). Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world

Federal Agency for Security in Information Technology (2000) IT Baseline Protection manual, October 2000, Germany, Available at: http://www.iwar.org.uk/comsec/resources/standards/germany/itbpm.pdf

ITIL v.3 (international) - IT Infrastructure Library - Global standard in the area of service management. Contains comprehensive publicly accessible specialist documentation on the planning provision and support of IT services. ITIL - IT Infrastructure Library, ITIL-ITSM, http://www.itil-itsm-world.com/ and http://www.itilofficialsite.com/home/home.asp

IETF RFC2119 (1997) This document specifies an Internet Best Current Practices for the Internet Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited. https://www.ietf.org/rfc/rfc2119.txt

ISACA – Business Model for InfoSec (BMIS) - http://www.isaca.org/Knowledge-Center/BMIS/Pages/Business-Model-for-Information-Security.aspx

ISACA - COBIT - Control Objectives for information and related technology - Generally accepted information technology control objectives for information technology. Covers effectiveness, efficiency, availability, integrity, confidentiality, reliability and compliance. http://www.isaca.org

ISACA – RISK IT Framework for Management of IT Related Business Risks - http://www.isaca.org/knowledge-center/risk-it-it-risk-management/pages/default.aspx

ISSA GAISP (2003) Generally Accepted InfoSec Principles GAISP v3.0, http://all.net/books/standards/GAISP-v30.pdf

ISF Standard of Good Practice – "Updated annually, the Standard of Good Practice for InfoSec (the Standard) is the most comprehensive InfoSec standard in the world, providing more coverage of topics than ISO. It covers the complete spectrum of InfoSec arrangements that need to be made to keep the business risks associated with information systems within acceptable limits, and presents good practice in practical, clear statements". Covers security management, critical business applications, computer installations, networks, systems development https://www.securityforum.org/tools/sogp/ The 2014 update features new guidance on: Cyber Resilience, Securing the Supply Chain, Mobile Device Security (BYOD), Data Privacy in the Cloud, Critical Infrastructure. The 2014 Standard helped management of information risk and enabled compliance with ISO/IEC 27002:2013, COBIT 5 for InfoSec and the SANS Top 20 Critical Security Controls. It also provided organisations with detailed controls which help compliance with the US NIST Cyber Security Framework and the UK Cyber Essentials Scheme.

ISO (2002) PD ISO/IEC Guide 73:2002, Risk Management – Vocabulary – Guidelines for use in standards

ISO (2004), PD ISO/IEC TR 18044:2004 Information technology— Security techniques — Information security incident management

ISO (2005) ISO/IEC 27001:2005, Information technology – Security techniques – Information security management systems – Requirements

ISO (2008) ISO/IEC 38500:2008, Corporate Governance of Information Technology, Geneva: ISO

ISO (2009) ISO/IEC 15408-1:2009; Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model

ITIL – IT service management infrastructure library, https://www.axelos.com/best-practice-solutions/itil

NFPA 1600 (2013) - Standard on disaster/emergency management and business continuity programmes. US National Fire Protection Association

O-ISM3 - is an InfoSec management maturity standard published by The Open Group, a leader in the development of open, vendor-neutral IT standards and certifications. http://www.ism3.com

OECD Guidelines for the Security of IS and Networks: Towards a Culture of Security – addresses laws, codes of conduct, technical measures, management and user practices, public education/awareness activities - http://www.oecd.org/sti/ieconomy/15582260.pdf

PCI Security Standards Council – payment card data security - https://www.pcisecuritystandards.org/security_standards/

SABSA – the world's leading open security architecture framework and methodology, business-driven, open and inclusive, readily integrates with other frameworks and tool such as ITIL, ISO27000 series, COBIT etc. It can be used as a compliance and governance framework for complex sets of standards. http://www.sabsa.org/

SANS Top 20 Critical Security Controls - https://www.sans.org/critical-security-controls/

SEI CMMI, Software Engineering maturity and measurement standards www.cmmiinstitute.com

UK Cabinet Office (2014) HMG Security Policy Framework - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/316182/Security_Policy_Framework_-_web_-_April_2014.pdf

UK CESG IA Maturity Model (IAMM) - https://www.cesg.gov.uk/policyguidance/IAMM/Pages/index.aspx

UK CESG Publication and Guidance available at: http://www.cesg.gov.uk/PolicyGuidance/Pages/index.aspx and http://www.cesg.gov.uk/publications/Pages/publications.aspx

US HIPAA Security Rule – Healthcare Insurance Portability and Accountability Act of 1996 (HIPAA) - http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/security101.pdf

US National Institute of Standards and Technology (NIST), Computer Security Division, Computer Security Resource Center, Special Publications - 800 series and others. Available at: http://csrc.nist.gov/publications/nistpubs/index.html. Many of these have been listed in the Bibliography.

Network Security Management Best Practice Resources

20 Critical Security Controls for Effective Cyber Defense http://www.sans.org/critical-security-controls/interactive.php

Build and Operate a Trusted Global Information Grid (GIG) - (another pictorial) - http://iac.dtic.mil/iatac/download/ia_policychart.pdf

Defence Signals Directorate (DSD) Top 35 Strategies to Mitigate Targeted Cyber Intrusions http://www.asd.gov.au/infosec/mitigationstrategies.htm

Kaeo, M. (2003) *Designing Network Security,* 2nd Edition, Cisco Press, http://www.ciscopress.com/bookstore/product.asp?isbn=158714249X

Enterprise Information Protection - Detailed table of contents is at: http://asp-press.com/1-878109-43-X/1-878109-43-X-TOC.pdf

Establishing Wireless Robust Security Networks http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

General Design Considerations for Secure Networks http://www.ciscopress.com/articles/article.asp?p=174313

The Global Information Grid (GIG) is an all-encompassing communications project of the United States Department of Defense: http://en.wikipedia.org/wiki/Global_Information_Grid

Improving Information Technology **-** http://www.auditnet.org/articles/DSIA201005.htm

NSO Quant: Monitor Process Map **-** http://www.securosis.com/projectquant/nso-quant-monitor-process-map

The Jericho Forum - https://collaboration.opengroup.org/jericho/index.htm

Network management presentation with a strong vendor focus http://www.netcraftsmen.net/component/docman/doc_download/221-network-management-best-practices.html

Network Security Architectures - http://www.ciscopress.com/bookstore/product.asp?isbn=158705115X

Network Security Auditing - http://www.ciscopress.com/bookstore/product.asp?isbn=158705941X

OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation) http://www.cert.org/resilience/productsservices/octave/

Open Web Application Security Project (OWASP) https://www.owasp.org/index.php/Main_Page

Open Web Application Security Project (OWASP) top 10 - https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

SANS InfoSec Reading Room http://www.sans.org/reading_room/

SANS Network Security Resources http://www.sans.org/network_security.php

Securosis Research - http://www.securosis.com/research *- includes a context pictorial*

The Psychology Behind Security https://www.issa.org/images/upload/files/Sternberg-Psychology%20Behind%20Security.pdf

The Art of War http://astore.amazon.com/corporategovernance-20/detail/1590302257

The Open Group Architecture Framework (TOGAF) http://www.opengroup.org/subjectareas/enterprise/togaf

Product Assurance

Common Criteria for Information Technology Security Evaluation. August 1999. [Accessed 1 March 2015]. Available at: http://www.commoncriteriaportal.org/

Commercial Product Assurance Certification http://www.cesg.gov.uk/servicecatalogue/Product-Assurance/CPA/Pages/CPA-and-other-schemes.aspx

http://www.tscheme.org/

http://www.crest-approved.org/

Paradigms

The following paradigms were identified in the research, to which i3GRC™ is now added:

CIA Triad
Parkerian Hexad
Defence in Depth
Keep it Simple, Stupid
Least Privilege
Need to Know
People, Process, and Technology
Prevention, Detection, Recovery, Response, Feedback (in an OODA loop)
Privacy by Design
Security by Design
Shewhart Cycle or Deming Wheel (Plan, Do, Check, Act)
RMIAS – Reference Model for IA and Security, 2014
i3GRC™ – new paradigm, 2015

Professional Qualification Resources

Certified Protection Professional (CPP) offered by ASIS International
Professional Certified Investigator (PCI) offered by ASIS International
Physical Security Professional (PSP) offered by ASIS International
Global IA Certification (GIAC) series administered by the SANS Institute
Certified Ethical Hacker (CEH) offered by the EC Council
Certificate in InfoSec Management Principles (CISMP) administered by ISEB/BCS
Certified InfoSec Auditor (CISA) offered by ISACA
Certified InfoSec Manager (CISM) offered by ISACA
Systems Security Certified Practitioner (SSCP) administered by (ISC)²
Certified IS Security Professional (CISSP) administered by (ISC)²
Certified Cloud Security Professional (CCSP) administered by (ISC)²
Certified Authorization Professional (CAP) administered by (ISC)²
Certified Secure Software Lifecycle Professional (CSSLP) administered by (ISC)²
Certified IS Security Professional (CISSP) administered by (ISC)²
Architecture (CISSP-ISSAP) administered by (ISC)²
Engineering (CISSP-ISSEP) administered by (ISC)²
Management (CISSP-ISSMP) administered by (ISC)²

Essential Body of Knowledge (EBK)

- Data security
- Enterprise continuity
- IT security training and awareness
- Network security and telecommunications
- Physical and environmental security
- Regulatory and standards compliance
- Strategic management

Digital forensics
Incident management
IT systems operations and maintenance
Personnel security
Procurement
Risk management
System and application security

Cyber Security Body of Knowledge (CyBoK) - https://www.cybok.org/

10.20 IA Definitions

Table 29 below provides a range of selected definitions of IA from the available sources, be they ***government (G), practice (P)*** and ***academic*** **(A)**.

	Definition	Source	Date	Title / Comments
A	Protection of information systems (IS) against unauthorised access to or modification of information, whether in storage, processing or transit and against the denial of service to authorised users, including those measures necessary to detect, document and counter such threats.	McCumber, J	October 1991	IS Security: A Comprehensive Model" in *Proceedings 14th National Computer Security Conference*
G	Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Assurance is not, however, an absolute guarantee that the measures work as intended. Like the closely related areas of reliability and quality, assurance can be difficult to analyze; however, it is something people expect and obtain (though often without realizing it). For example, people may routinely get product recommendations from colleagues but may not consider such recommendations as providing assurance.	NIST	October 1995	An Introduction to Computer Security: The NIST Handbook Special Publication 800-12
G	Information operations (IO) that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation; including providing for restoration of IS by incorporating protection, detection and reaction capabilities.	*U.S. DoD 3600-1* *Maconachy*	1996 2001	Debra S Hermann (2002) refers to this but leaves out the *confidentiality* word. **First available definition of IA, covering the Five Pillars of IA – availability, integrity, authentication, confidentiality, and non-repudiation (so CIA+)**
G	IO [measures] that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection and reaction capabilities.	*IS Security (INFOSEC) Glossary, NSTISSI No.4009,* CNSS Instruction 4009 SP 800-59	August 1997	Originally The National Security Telecommunications and IS Security Committee (NSTISSC) and the Committee on National Security Systems (CNSS) – became the "National IA Glossary" - IA is a subset of IO – NOT a subset of InfoSec. *It differs from* ***security assurance****, because the focus is on the threats to information and the mechanisms used to protect information and not on the correctness, consistency or completeness of the requirements and implementation of those mechanisms (Brown and Topi, 2003).*

G	**InfoSec.** Information security is the protection and defense of information and IS against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. **Information assurance.** Information operations that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection, and reaction capabilities. Also called IA.	US DoD Joint Publication 3-13, Definitions included in Joint Pub 1-02 US DoD	9 October 1998 2007	US DoD (1998) *Joint Doctrine for Information Operations*, Joint Publication 3-13, Joint Chiefs of Staff, 9 October 1998 updated 27 November 2012 and 20 November 2014, [Accessed 13 September 2015]. Available at: http://www.dtic.mil/doctrine/new_pubs/jp3_13.pdf
G	**InfoSec:** The protection of information and IS from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. Protecting information and IS from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— 1. **integrity**, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; 2. **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and 3. **availability**, which means ensuring timely and reliable access to and use of information.	SP800-18; SP800-37; SP800-53; SP800-53A SP800-60; SP800-66 FIPS 199; FIPS 200; 44 U.S.C., Sec 3541 44 U.S.C., Sec. 3542	1998 2004 2005 2008 2008 2004 2006 2002 2002	NIST publications, available here http://niatec.info/ViewPage.aspx?id=241 FISMA – Federal InfoSec Management Act 2002
G	**IA** - Measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of IS by incorporating protection, detection, and reaction capabilities. Also called **IA** (JP 3-13). **IA —** Actions that protect and defend IS by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. Also called **IA** (JP 3-12).	US DoD Joint Publication 1-02 CNSSI-4009	2001 2010	Dictionary of Military and Associated Terms through to 2009 Updated in 2010 through to 15 June 2015 Inextricably linked with IO
P	**IA** is a holistic approach towards protecting information and IS by ensuring availability, integrity, authentication, confidentiality, and non-repudiation. Although building on the discipline of InfoSec, the concept of IA raises the profile of security as a business critical operational function rather than as a technical support function.	IAAC	2002	Protecting the Digital Society: A Manifesto for the UK, March 2002

A/P	**IA** is a management process, the purpose of which is to ensure that the critical information within an organisation and the systems and networks that manage it are reliable, secure and private, and that measures and processes are in place to counter malicious electronic based attacks. IA encompasses other disciplines such as InfoSec management, risk management and business continuity management. 'IA goes beyond Business as Usual InfoSec as it is particularly concerned with high-end threats to systems that are critical not only to the enterprise but also to the wider national or international information infrastructure.'	IAAC	17 March 2003	Andrew Rathmell, Benchmarking IA in the Tele-communications Sector)
G	**IA** (IA) – the confidence that IS will protect the information they carry and will function as they need to, when they need to, under the control of legitimate users or the confidence that IS will function when and as they need to, are controlled by legitimate users and protect the information they handle There are five key principles, essential for safe electronic transactions: 1. **Confidentiality** – keeping information private 2. **Integrity** – ensuring information has not been tampered with 3. **Authentication** – confirming the identity of the individual who undertook the transaction 4. **Non-repudiation** – the individual who undertook the transaction cannot subsequently deny it 5. **Availability** – ensuring information is available when required. IA is about meeting these requirements.	UK CSIA	June 2003	UK Government Strategy for IA
P	**Assurance** – measure of confidence that the security features and architecture of a system accurately mediate and enforce the security *policy*. The policy need not be tied solely to issues of *confidentiality*, but may address requirements for *availability*, *integrity* of data or processing, *reliability*, safety or other factors. Assurance is often neglected in planning for security: each security function should have an assurance requirement or metric. Assurance may result from formal methods, or it may be partially determined by *audit, penetration testing, simulation,* testing or third-party reviews.	Slade, R.	2006	Dictionary of InfoSec
P	**IA** is the confidence that the information assets with an organisation are reliable, accurate, secure and available when required. IA includes Information held in every form (IS, on paper, other records, speech). It embraces IM, including InfoSec management, information and records management, data quality, data protection, privacy (because of close	IAAC	2006	*IA in a Global Bank*, presentation to BCS Birmingham IT Security Conference, June 2006, HSBC Holdings plc

	confidentiality links and Organization for Economic Co-operation and Development [OECD] guidance requirements) and physical protection. It includes aspects of corporate governance, risk management and business continuity (resilience) and ensures that information is fit for purpose.			
A	**IA** is ensuring that your information is where you want it when you want it, in the condition that you need it and available to those that you want to have access to it – but only to them.	Blyth, A. and Kovacich, K.L.	2006	IA, Security in the Information Environment
P	**IA** is about the protection of information, based around what we traditionally understand as InfoSec. It has at its core the principles of CIA. However, IA reaches beyond this and explicitly connects with the concerns of the organisation by embracing the broader disciplines of risk and business continuity management.	UK BCS	2007	Article by Debi Ashenden – representing both IAAC and BCS
P / A	**IA** defines and applies a collection of policies, standards, methodologies, services and mechanisms to maintain mission integrity with respect to people, process, technology, information and supporting infrastructure. IA addresses information, not just information technology. A chief information officer (CIO) is responsible for information, not just information technology. IA provides for *confidentiality, integrity, availability, possession, utility, authenticity, non-repudiation, authorized use* and *privacy* of information in all forms and during all exchanges.	Willetts, K.	2008	Willetts took the original IA definition, enhanced it with the Parkerian Hexad and created an IA Architecture - IA^2
P	**IA** - The term used to describe confidence in the processes of IRM.	IPS	April 2010	Draft Identity Rights Charter for consideration from the IPS Expert Panel - a thin representation....
P	**IA** is the preservation of confidentiality, integrity and availability of information. • **Confidentiality:** confidential information must only be accessed, used, copied, or disclosed by users who have been authorised, and only when there is a genuine need. • **Integrity:** information must be protected from unauthorised access or revision, to ensure that the information is not compromised through corruption or falsification. • **Availability:** the information, the computing systems used to process the information, and the security controls used to protect the information must all be available and functioning correctly when the information is needed.	Withheld	2015	Well known and respected UK security consultancy [This has to be highlighted as being a blatant and direct relabeling of **InfoSec** (the CIA) as **IA** and is therefore, by virtue of its existence in client reports, **wrongly** educating current generations of clients, private and public sector bodies and future IA professionals. This is the reason for this research study.]

Table 29: IA Definitions

10.21 UK Public Sector IA Reporting 2007-2008

Independent Police Complaints Commission Independent Investigation into the HMRC loss, 61 pages (IPCC, 2008);

Kieran Poynter Review of InfoSec at HMRC, 109 pages (Poynter, 2008);

House of Commons Justice Committee Protection of Private Data Report, 28 pages (UK House of Commons Justice Committee, 2008);

Sir Gus O'Donnell Data Handling Procedures in Government, 46 pages (UK Cabinet Office, 2008b);

Nick Coleman Protecting Government Information - Independent review of government IA, 31 pages (Coleman, 2007);

House of Commons Home Affairs Committee Report on Surveillance Society, 119 (main report) + 281 (supporting report) pages (UK House of Commons Home Affairs Committee, 2008);

Sir Edmund Burton, Final Report into the loss of MoD Personal Data, 76 pages (Burton, 2008);

MOD Action Plan in response to Burton Report, 28 pages (UK MoD, 2008);

House of Commons debate on Data Protection held on 12 June 2008 led by Baroness Miller of Chilthorne Domer, 31 pages (Miller, 2008);

Ministry of Justice Data Sharing Review, Richard Thomas, the Information Commissioner, and Dr Mark Walport, Director of the Wellcome Trust (Thomas and Walport, 2008); and

Review of Criminality Information – Sir Ian Magee (Magee, 2008).

The reason for referring to the number of the pages (where available) in the above reports is to highlight how much has been written around the subject area.

11 APPENDIX II: CASE STUDY RESEARCH

11.1 Public Sector Case Study – GCSx [CS1]

11.1.1 The researcher was engaged as a consultant security programme manager to assist a north east UK Council to achieve the government code of connection (GCSx) accreditation in order to maintain sensitive system connectivity. The process was formulaic in nature with particular gateways to be passed, and continues to this day in various iterative versions. At the time of joining the organisation, the Researcher ensured that sufficient background historical understanding was gained in order to ensure that any implementation plan created would achieve the required outcomes through successful design. This history is provided in Table 30 below.

Date	Description	Comments – what the researcher identified
06/05/97	Finance and General Purposes Sub-Committee paper entitled "Information Technology – Contingency Planning and Disaster Recovery"	"ICT Services are planning to introduce best practice notes during the course of 1997/1998 to aid departments to consider the issues involved". None have been specifically evidenced. Sadly the copy available stated "never sent" at the top.
25/06/97	District Audit Network Risk Assessment sent to xxxxx *(Strategic Review ongoing at the time – 20 years later and little had changed)*	Lack of a defined and tested DR Plan mentioned Lack of security, fault and performance management on the Network Lack of standards, procedures and guidance for everyone to follow ICT Audit states that "activities of the Risk Assessment are a cause of concern".
10/99	External company – Risk Management Review of Council Computer Systems	References issues with Backup, Disaster Recovery, implementation of Risk Management Cases for new systems……
12/06/00	External company costs for assessment of the Council against BS7799:1999	The Council were considering certification to the then British Standard for InfoSec Management Systems (BS7799 – now an International Standard ISO 27001).
06/11/02	BS7799 Registration Project	A BS7799 PID was created but this project did not appear to have been followed through.
06/11/02	Council Policies and Principles Manual includes InfoSec	Based on BS7799-2:2002 and follows its structure in its entirety.
06/11/02	Detailed Application Risk Analysis	Process and template prepared by internal employee responsible – not completed, embedded or shared.
06/11/02	Council Homeworking Detailed Risk Analysis v1	Document completed but no evidence of actions being followed up

? 2003	External InfoSec course reviewed	Presumably with a view to it being embedded and available within IT Services and beyond – it included discussion/education about information classification…..
26/06/03	Data Risk Analysis v1	Risk Management Process documented, with an Owner – but no evidence of it having been used / completed / shared.
26/06/03	Detailed BS7799 Action Plan	Owned document, incomplete. If this had been followed up and completed the CoCo would have been easily achieved in a timely manner – instant responses would have been available and the BS7799 certification would have been evidence enough.
27/06/03	Council InfoSec Action Plan	Covering all aspects including InfoSec Policy and Infrastructure but Personnel and InfoSec Awareness sheets were blank/empty of tasks. Utilised an external company to assist in the completion of the tasks.
03/ and 04/07/03	Asset Inventory and Risk Assessment done	A comprehensive Risk Analysis was carried out on the IT Asset Inventory
11/08/03	Corporate Business Continuity Planning introduced	Internal Information Asset owner offered to workshop with ICT to develop the appropriate Service Level BCP. BCP Guidance Notes prepared (dated June 2003).
18/02/05	**IA** CD received from CESG	Part of an effort to extend advice given to central government to provide benefit to the wider public sector.
17/10/05	Second Edition Of **IA** Guidance For The Wider Public Sector CD received from CESG	Includes IS2 – providing policy and guidance on the risk management and accreditation of IS.
Feb 07	ISO 27001 Audit Report (internal)	Audit carried out in December 2006, reflecting that in 2004 significant progress needed to be made and a previous audit was thus abandoned. Work commenced in 2003 was not progressed and no progress was made since. The audit report said progress and likelihood of achieving the Standard was “adequate” yet a current, up to date copy of the standard was not present or available at the time. Ethically challenging reporting.
01/04/08	Government Connect (GC) letter to all LA Chief Executives	Signed by all GC strategic partners – requesting that Chief Executives champion their authorities early adoption of GC

01/04/08	GC letter	GC becomes a **cross government programme** - GC stated as being a "key strategic enabler to improving public services for citizens and communities".
June 08	Audit of ICT Network Security – Action Plan	Security roles to be clarified through job descriptions in new structure – committed to by Ian Cooper with a target date of **December 2008** "A policy on the connection of non-standard equipment to the network should be determined following an investigation into the feasibility of a cost effective method of locking out any non-Council/approved equipment be undertaken". Rejected due to the potential user disruption and amount of work generated as a result.
07/07/08	GC letter to all LA 151 officers	Advising of DWP revised Data Access Policy
22/07/08	Telephone call from DWP	DWP requesting Council place an order for connection
18/08/08	GC letter to LA 151 officers	Detailing exemption process.
22/09/08	Strategic Performance Management Group	Agenda item – ICT Owners briefed service reps on GC
29/09/08	Business Case submitted	BC to outline requirements
29/09/08	HCC letter signed by 151 officer	Request for exemption from DWP data access policy until 30/09/09 – Gareth Baker then had *two weeks* to produce a Code of Connection submission return to Government explaining what HCC was doing to meet the 92 requirements.
24/10/08	GC letter to 151 officer	Exemption request approved.
07/11/08	DWP letter to LA Housing Benefit section	DWP memorandum of understanding.
03/12/08	GC letter to LA 151 officers	Advising of DWP file transfer arrangements
03/12/08	PSF article on Remote Working	CoCo controls *preclude* remote workers from using their own PCs at home, **even** when using a secure virtual desktop, thus requiring LAs to supply staff with council-controlled equipment.
22/01/09	Land Registry e-conveyancing Portal Guidance notes produced	Arrived **November** 2009 - Land Registry Direct (LRD) would begin to be turned off from ***January 2010***
02/02/09	Land Registry Full Network Access Agreement produced	Arrived **November** 2009 - Land Registry Direct (LRD) would begin to be turned off from ***January 2010***

Mid 02/09	Guidance issued from Govt Dept BIS re ELMS - Electronic Licence Management System	First heard about it on ***15th December 2009*** with a lead time of two weeks to implement by the deadline of **28th December 2009**.
05/06/09	GC Project Team Minutes	First meeting took place where DWP Access Policy was discussed and the implications of the work ahead to achieve the project.
08/06/09	Business Case submitted	Revised BC to CAB to secure funding. Finally, resources are made available and a project is instigated that has to operate under stressful conditions due to the tight timescales afforded.
05/08/09	GC Project Team Minutes	First mention of 8 character password requirement for all.
Mid 08/09	More guidance issued from BIS to LA's ref ELMS	New bank account to be set up? Contact details provided for the four main suppliers. Who dealt with this and got on with the actions contained therein? First seen by ICTEG on ***15th December 2009***.
07/09/09	Cabinet Office letter sent to Section 151 Officer referencing change from version 3.2 to version 4.1 of CoCo	Council have until **May 2010** to comply with the updated controls where a significant number have shifted from "should" to *"must"*. This includes the mandatory protective marking of emails (for which a technology bid was put into the GC The Sequel Business Case – but rejected). [GCSx project team only made aware of this letter on *7th December 2009* – letter went "missing in action" in the Council.]
23/09/09	GC Tech Team letter confirming successful GCSx connection	Despite some people's cynicism, the project was successful and Revs&Bens achieved the required connection. However, the snagging list was significant as a result of the "rushed" nature of the project. This was compounded by the central government *expectation* that "connected" meant "the whole Council" rather than the then segmented network which therefore needed to be rolled out to the whole Council.
05/10/09	"GC The Sequel" commences	Immediately recognising the above need to roll out to the wider Council, a business case was put together.
26/10/09	Final version of GC the Sequel presented to CAB for approval.	£2.6m too steep for leadership but there was acceptance that the work still needed to be done and that CST needed to accept this as a Council wide issue rather than an ICT specific project. It is about protecting *information* not bits and bytes, as such.
06/11/09	Secure Infrastructure CST Briefing 061109	Hard hitting CST report delivered – in order to ensure that CST understood the key messages and requirements across the Council. Determined to bat this back to ICT and highlight that ICT *should* have brought the issues to the service areas to ensure that *they* factored them into their planning for 2010 onwards, rather than the other way around.

		This is a frustrating stance to take, given that the central government departments relevant to each service area will have been mentioning the usage of the GCSx for secure communications ongoing and are expecting and anticipating that this is in place already.
17/11/09	Implementation Plan for CST	Prepared as requested – along with a number of other spreadsheets and reports to fulfil a determination to put off the inevitable.
17/11/09	ICT CAB agree in principle to the now reduced £616k project bid	Agreement in principle reached to at least move onto a Phase 3 implementation which allows for training up all relevant users across the Council and delivering the necessary secure connectivity to Children & Young People (CYP), Streetscene, Citysafe etc.
10/12/09	ICT CAB ……	Weeks lost in an internal political wrangle creating reporting documents to reflect history rather than preparing and planning properly for the future. In the meantime the day to day project management suffered because it is impossible to be all things to all people – including attempting to meet the demands of service areas wanting to be connected next on a daily basis as the momentum grows despite the negativity from the top.

Table 30: Public Sector Case Study Historical Chronology

11.1.2 By January 2010 the Council leaders came to an agreement and the project limped forward. Amongst other successes, an organisation wide password change programme was implemented; the political landscape changed again; the ongoing Code of Connection continued; thousands attended face to face interactive InfoSec awareness sessions but the money ultimately ran out for external support and the Researcher was let go.

11.1.3 The reason for sharing another chronological listing is to provide further evidence of a core tenet of this study. The greater challenges faced by IA practitioners are invariably managing organisational politics, culture, team dynamics, rather than implementation of technologies per se.

HM Courts Service staff breached government database of personal information

Staff working for Her Majesty's Courts Service have breached security on the government database that stores personal data about everyone in the UK. Freedom of Information requests by Computer Weekly also revealed that the Department for Work and Pensions (DWP) caught 124 council workers and sacked 24 of them for breaching security on the Customer Information System (CIS), which, with 90 million records, is one of the largest databases in Europe. Email exchanges by IT security staff at the DWP and the Ministry of Justice also expose the weak grip the DWP had on the security of the five-year-old CIS database. (Ballard, 2010)

11.1.4 In the researcher's experience, this was another organisation that benefited greatly from a positive engaging communication style actively encouraging participation ensuring employees willingly attended awareness sessions and shared their issues during and afterwards to maintain momentum for the wider IA improvement and reporting required. All efforts were resonant far beyond the ICT department itself and indeed beyond the local council to other related public sector bodies in order to leverage learning and share best practice.

11.1.5 Within the context of the political domain, something keenly felt by Local Authorities, a number of key systems were in need of connection to the GCSx and there were obvious instances of system creation and system decommission which implied tax payers money had been wasted leading to a lack of trust by local citizens for "big government" IT projects, including a sense that the work done was building up a privacy deficit for future generations.

11.1.6 In another example of the challenges faced by the public sector at the time, Fire Stations were to be considered to be "community" spaces and thus the public could freely enter at any time (in any numbers). This would create physical security challenges needing new solutions: keys could be out on desks, that would need to be put in cupboards etc; data and information would need to be similarly safely stored away; all computer screens would need to be always locked; a clear desk policy would be required for all. These were significant challenges given that physical and InfoSec were, at the time, lax at a local command post level.

11.1.7 For the Poll tax system at the time, a well-known public sector IT provider had charged back the Local Authorities for change requests to a system that they had designed wrongly. It was a head tax but the system was set up to collect property details, which was excessive data collection. This behaviour created a waste of public funds, on many levels. The Complexity of these systems was not lost on the Researcher given that the better gains were to be had from greater synergy between systems, with improved data sharing.

11.2 Private Sector Case Study – Services [CS2]

11.2.1 The Researcher was asked to join the organisation and address Security Policy gaps. In so doing, taking a purist view of what should be in place for a large organisation providing services to multiple clients worldwide with competing and complex global regulation, legislation and industry standards. Multiple deficiencies were found which, to reveal and discuss, would create further organisational risk and vulnerabilities. Size and scale made for a cumbersome and thus lengthy change process. The work required was beyond that of both InfoSec and IA, requiring greater alignment in the governance space, involving outreach across the whole organisation.

11.2.2 Over the course of the intervening three and a half years, the Researcher was promoted to a Chief InfoSec Officer role with global influence. A UCF was created in order to standardise the ability of the company to respond to external requests for assurance of compliance against the aforementioned multiplicity of requirements. The organisation operated multiple (largely compliance only) ISMS – and required the Researcher's i3GRC™ approach to unify for the sake of the global organisation and its reporting and thus for sense for its many international clients – and the different regulators requiring evidence.

11.2.3 The outcomes of the work are captured in the briefing paper provided at **Section 10.3** below. This was created for submission to a Technical Conference early in 2015 and helped to provide focus for the team, internal customers, external customers and organisational leadership.

11.2.4 The tool was used as a global Account and Business Unit framework for:

- *Mapping security policy to legislation, regulation and industry standards*
- *Defining security control requirements*
- *Defining compliance landscape*
- *Assessing compliance landscape*
- *Assessing risk(s)*
- *Recording Findings (from any source event)*
- *Recording Exceptions to Policy*
- *Recording Operational Risk(s)*
- *Recording Audit evidence centrally*
- *Reporting pan ES compliance, security, risk status*
- ***Common platform, repeatable results***

11.2.5 Figure 88 represents the scope of Archer eGRC modules available in the platform.

Figure 88: Archer eGRC Graphic

- ***Policy Management*** *– Centrally manage policies, map them to objectives and guidelines, and promote awareness to support a culture of corporate governance. Single source policy set solution to house mapped global corporate policy content to Archer content with automatic links to 47 Regulations/Industry Standards.*

- ***Enterprise Management*** *– Manage relationships and dependencies within your enterprise hierarchy and infrastructure to support GRC initiatives. Single source rollup view into Assets, Client, Contract, Account and Infrastructure information.*
- ***Risk Management*** *– Identify risks to your business, evaluate them through online assessments and metrics, and respond with remediation or acceptance. Customizable Account risk assessments, Risk ratings rolled into multilayered Dashboards to support the organisation.*
- ***Compliance Management*** *– Document your control framework, assess design and operational effectiveness, and respond to policy and regulatory compliance issues. Standard customizable Self-Assessments, Compliance ratings rolled into multilayered Dashboards to support the organisation.*
- ***Issue Management*** *– Single source for all Findings, Remediation Plans, and Exception to Policy records, correlated to Account/Infrastructure across the organisation.*
- ***Audit Management*** *– Centrally manage the planning, prioritisation, staffing, procedures and reporting of audits to increase collaboration and efficiency. Increased functionality for tracking Audit Events and Findings.*
- ***Threat Management*** *– Track threats through a centralized early warning system to help prevent attacks before they affect your enterprise. Threat/Vulnerability Intelligence Clearinghouse, integrated Vulnerability Scanning provides associated view of overall risk and compliance posture.*
- ***Incident Management*** *- Report incidents and ethics violations, manage their escalation, track investigations and analyze resolutions.*
- ***Business Continuity Management*** *– Automated approach to business continuity and disaster recovery planning, and enable rapid, effective crisis management in one solution. Storing Business Impact Assessment results to correlate against risk assessments and action plans.*

11.2.6 Another label used for internal marketing purposes was that of FREIA - because once fully built, Archer would house relevant **F**indings, **R**isks, **E**xceptions, **I**ssues and **A**ssessment requirements.

11.2.7 The Risk Management module is intrinsically linked with other modules in the Archer Suite:

- *Policy Management*
- *Enterprise Management*
- *Audit Management*
- *Compliance Management*
- *Threat Management*

11.2.8 The integrated workflow and combined intelligence increases:

- *Visibility*
- *Collaboration*
- *Efficiency*
- *Accountability*

11.2.9 Figure 89 represents the benefits of implementing a full eGRC platform.

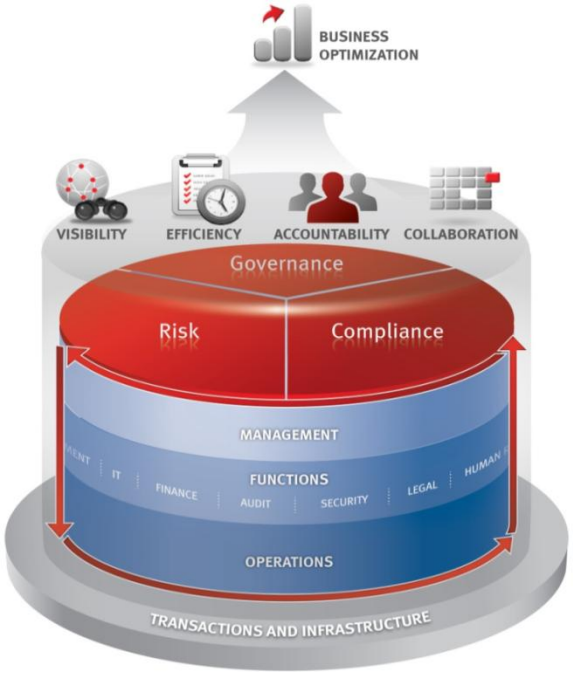


Figure 89: eGRC End to End Implementation Model

11.2.10 Figure 90 presents the High Level Solution Overview for full eGRC implementation:

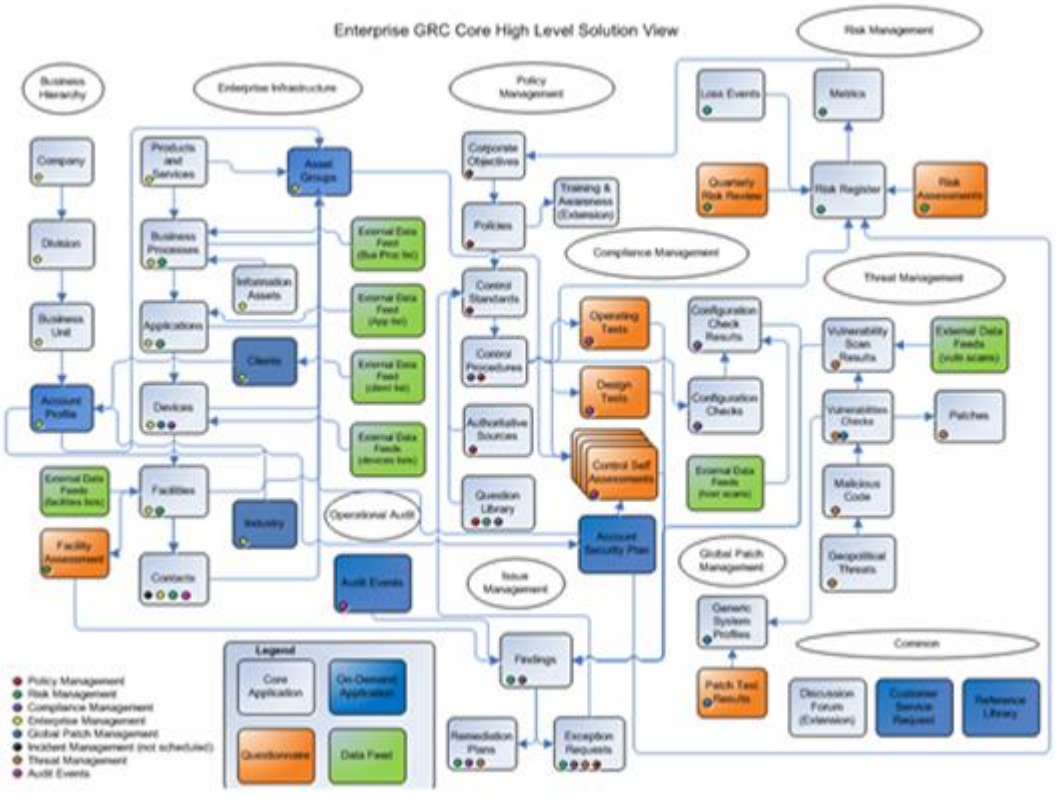


Figure 90: eGRC High Level Solution View

11.3 HEART – a Technical Research Conference briefing paper

HEART – Holistic Enterprise Assurance, Risk and Trust – …… providing "a safe pair of hands"

Author(s) Names - *removed*

Abstract

Sustainability of an organisation's security posture in the future requires an understanding of the need to balance risk and opportunity – without visibility of either, the ability to thrive is less effective and more challenging given the volume of uncertainty. For too long, the security approach has been one of addressing the Compliance portion of Governance, Risk, and Compliance (GRC) initiatives. This new approach moves the emphasis back to the G and R – Governance and Risk - in order to better position the organisation for future resilience. As a global service provider, the Company has a constant need to be aware of the many threats and vulnerabilities that may affect our clients. The ability to assess the potential impact of these is vital. The vectors are sporadic and extensive and originate from the many crises facing the world today. The challenge is to have available to our account teams the necessary information to allow for sufficient oversight to be assured that any threat facing a client can be risk assessed and managed through the effective implementation of appropriate controls on each and every occasion. We have directly met this challenge by implementing a solution that gives us visibility of all assets – by leveraging a proper configuration management database (CMDB), linked to various feeds of data relating to device health and network performance and threat landscape. This is supported by the creation of a new legislative, regulatory, industry value standard and geography landscape vectors that help to position the data for priority and impact. Together this will enable the Company to operate in a more agile and resilient manner, as a business as well as for all clients, through greater visibility of account risk and health status per region, per geography and per industry sector.

Problem statement

FY14 has so far reported 1,367 data breaches and more than 63,000 security incidents in 95 countries[1]. Mid-year 2014 data breaches exposed over 502 million records, far exceeding the mid-year point in 2013, the previous all-time record setting year.[2] Corporate espionage is on the rise. The maturity of CNE – Computer Network Exploitation – will be realised in the near future. Hacked stolen credentials led the way as the root cause. The Company handles the *largest volume* of credit card data worldwide – by a factor of **billions.** It is vital for the Company's Leadership Team (LT) to provide ongoing assurance to its customers that the Company is providing them with a secure environment; we *must* secure our customers data, information assets and intellectual property - maintaining an effective and appropriate "safe pair of hands". Currently, most accounts do not have a "one view" of their landscape and instead must go to many locations to "pull" data sets and seek to correlate the data points effectively enough to understand whether their client is at risk or not. This can only be identified through a combination of knowledge across the information assets we are charged to protect for our clients, the timeline within which they expect us to update those assets (network devices, firewalls, servers etc), the service level(s) they expect us to maintain and our ability to do so. This is made all the more challenging through the Cloud environment where the risk of design flaws affecting the safety and security of the information are paramount. There is also a need to build security into Enterprise Reference Architecture ensuring consistency of implementation of

[1] http://www.verizonenterprise.com/DBIR/2014/insider/
[2] http://datalossdb.org/

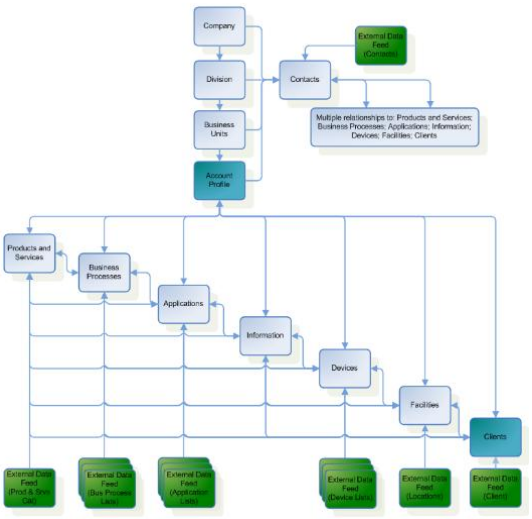
required controls so that we can demonstrate the appropriate Governance, Risk, and Compliance (GRC) throughout the lifecycle of the design, build, manage and maintain processes, end to end. We have previously lacked the ability to do this because we did not have a fully operational, mandated global corporate tool available for collation and reporting of the required information. We have had *multiple* toolsets – threat intelligence, security incident and event monitoring, security operations centres – all collating data at the node level. None of this has been collated and analysed in such a way as to present a holistic picture that best represents what most concerns executive leadership.

We are also subject to consistent ongoing findings with regard to Identity and Access Management (IAM) which, alongside Asset and Inventory Management (AIM), require significant global consolidation of processes and information sources to reduce risk.

Our solution

The Company Enterprise Security Information System (ESIS) Next Generation (NG) platform (built using the RSA Archer application) expansion through FY14 and across FY15 includes enhancements that extend the current reach, adoption, use, coverage and value of the tooling across the global enterprise. The fundamental premise of the solution is to provide ES executive leadership with a true view of global risk – through the provision of a collation service for multiple data feeds generating a central repository for key information points required to assess and manage risk. This is security intelligence at the macro rather than the micro level – across the whole GRC landscape. ESIS NG will take the data currently housed on multiple global SharePoints under the guise of the ASGCM – the Account Security Governance and Compliance Management dashboard – and replicate this, with improvements and enhancements in a fully supported and backed up enterprise management system, with global repository capability and appropriate executive management reporting functionality providing an effective risk context – to creative a robust Account Infrastructure Profile (AIP) for all accounts, business units, data centers etc. This will utilize feeds from other corporately available sources - including Salesforce.com, ArcSight, RTOps, Ticketing, ESM, Redfish, CMDB, Aries, ADMS, ESL – in order to best represent a number of key elements for the full enterprise: risk to the business; risk to the clients; opportunity to the business.

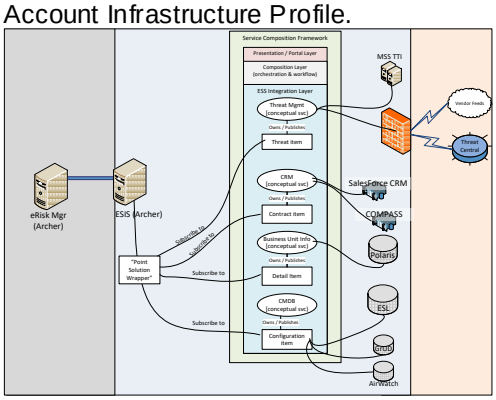
RSA Archer is an industry-leading eGRC tool, as defined by the Gartner Magic Quadrant. EDS purchased this tool, when Archer was a start-up company, and became one of their first customers. The tool itself is highly customizable, based on an SQL backend database, with multiple "modules" that can be purchased, to address various needs: Security Operations, Incident Management, Vulnerability Management, Risk Management, Policy Management, etc. The Company CISO team has mapped extensive content libraries, including standards and frameworks as well as regulations to the Company Security Policy framework. This provides a robust and comprehensive InfoSec management system from which the organisation can evidence its compliance with a multitude of international standards and regulations including ISO 27001 certification, PCI DSS compliance, NIST guidance and US Federal regulations. Given the current lack of ability to effectively present risk to the Company LT, the resulting capability to do so will be a significant governance enhancement providing real, transparent evidence of the much vaunted "safe pair of hands". The work the team has done so far will be invaluable to the Separation team as the larger global corporate entity separates into two separately traded companies. There will be an even greater need to have multiple sets of data for multiple parts of the global business – all requiring



knowledge of contracts signed; services sold; legislative framework; regulations and industry standards requiring compliance evidence and monitoring. This will provide all parts of the organisation with heat maps of opportunity, as well as reducing duplication of effort and reporting, as the teams coalesce and streamline operations.

Evidence the solution works

For the purpose of this TechCon brief, the AIP module is our customisation of the Enterprise Management Module – which is designed to catalogue assets as well as basic customer data and provides an overlay of intelligence to generate opportunity heat maps as well as account security health status. Our customisation takes this a step further by linking the asset data to an Account Infrastructure Profile.



As of the writing of this brief, we have built out the design of the AIP module in Archer using static data sets. The development team is working through the creation of records based on regular manual reports; the goal being to automate as much of the data loading as possible, over time.

The largest benefit of the solution is realised once all of the other modules are built out. The Policy module has been the initial focus as that provides the ability for Archer to perform risk scoring. The provision of data sets from Salesforce.com, the composite CMDB (called ESL), and business unit hierarchy (Polaris) are primary objectives for FY15. Additional data feeds on the roadmap may include: ArcSight, Airwatch, and ThreatCentral (crowd-sourced threat intelligence). The graphic shows the architectural roadmap for integration of the automated data feeds.

Competitive approaches

The enterprise GRC platform market has matured to a strategic focus on enterprise risk management and business performance. The next market phase includes integrated performance and risk management, industry- and function-specific applications, and mobility. Taking into account this maturity and the increasing professional expertise of GRC users, the CISO office has been applying its expertise to developing areas of the tooling which no other organisation is addressing, nor currently capable of achieving. Intellectual property is being utilised to create an extensive legislative landscape view within the Enterprise Management Module (the Account Infrastructure Profile) being built to provide this global view for all accounts. What the Company CISO team have done with the Archer technology (ESIS) and the reporting and visibility capability this will provide for an organisation with the global scale and magnitude of the Company, is **not** available anywhere else in the market.

Current status

The Policy Management solution is currently in beta testing in the Company and throughout FY15 will see month on month progression as we build out the profiles for all identified Company accounts, as well as Data Centres and business units and roll out Risk Management (to maintain comprehensive Risk Registers for every Account, Client, Business Unit, Organisation, Group, Data Centre across the global organisation). This will enable us to report per region, per geography, per industry sector on risk and account health status for the Company. The biggest challenge – working with others and attempting to abide by the global corporate approach, in transition to two separate trading entities throughout FY15.

Next steps

Once ESIS NG has been built out and contains all the required information points of the company, "GRC as a Service" is the next part of the development roadmap. The ability to harness this tooling to effectively provide a mirror service: both reassuring the Company LT and global corporate leadership that the Company has its landscape under control and is managing its daily operational risk environment effectively *and* providing the same visibility through

appropriate reassurance to the client landscape, external auditors and beyond as required. $3m estimated annual savings, plus $1m annual dollar value of future opportunity (minimum), plus $6m available spend from USPS due to US Fed support of use of Archer technology for GRC purposes. The development of this approach will provide the organisation with a unique market leading position to move the GRC tooling landscape forward but also the InfoSec management industry. This is the perfect marriage of *process* and *technology* with the *people* being supplied by a team of intelligent, innovative company employees!

References

http://www.emc.com/security/rsa-archer-governance-risk-compliance/index.htm
http://uk.emc.com/security/rsa-archer-governance-risk-compliance/index.htm
http://gcn.com/articles/2014/09/03/archer-rsa-cdm.aspx
http://www.csg.ethz.ch/education/lectures/ManSec/HS2013/Quadrant

NOTE: adapted from an original internal paper for a Technical Conference (TechCon) which was also utilised with external lawyers to validate the suitability of the programme of work for patentability of the software enhancements. Therefore, this information is commercially sensitive and has been edited. References are not in Harvard style as this paper is "as presented".

12 APPENDIX III: IA – A Chronology

12.1 Overview

12.1.1 This began as a UK specific endeavour but, through the course of the research, the scope of review broadened to include references to IS related events across an extensive timeline to evidence longevity of intention and purpose. In reviewing the contents, it is possible to trace the history and influence of a number of interrelated information themes

12.1.2 The researcher believes that as a result of the volume of available material, there is evident a plethora of confusing descriptions and explanations and it is only as a result of an exercise of chronologically recording and reviewing the history of how each ontology has been used, that there can be hope of addressing the skills crisis risking the success of the professionalism of IA.

12.1.3 It is possible to categorise a number of era as below:

- *1986-1991 Era of discovery*
- *1992-1998 Era of transition*
- *1999-2005 Era of fame and glory*
- *2006 onwards Era of mass cybercrime, cyber espionage, state sponsored espionage, digital espionage utilising computer network exploitation (CNE)*

12.1.4 These era could also be represented as per Figure 91 below

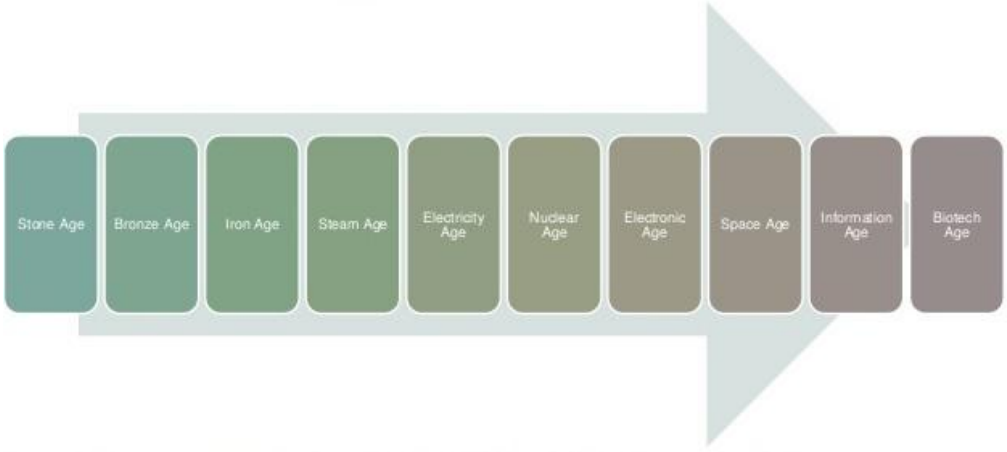


Figure 91: Technology Era

12.1.5 These map to the more commonly understood Industrial and Information era. Ogren and Langevin (1999) articulated the era as "Security epochs":

- *Revolutionary War to the mid-1820s, mid 1830s - 19th century ended with WW1*
- *WW1 and Soviet Union emerging*
- *1920 to 1946 global recession, rise of international communism as Europe collapsed – leading to American democracy crisis*
- *Cold War*
- *Information age – technological developments, chemical and biological weapons etc*
- *Cyber Security …. IoT*

12.1.6 These issues affect everyone, worldwide. Automating broken processes in the Information era, in order to achieve the IoT requires greater foresight to ensure IA is built in. The Foresight era is where we find ourselves now – with sufficient information available and easily accessible to distil enough knowledge to advocate appropriate change in order to design a safer and more secure future. For the key events that stand out over the last few decades (11 September 2001 – USA; 7 July 2005 – London; 7 January 2015 – Paris; 13 November 2015 – Paris; 22 March 2015 - Brussels) – the historical reflections are that the information was available but the intelligent analysis of it was not done in time to realise the benefits of the available knowledge and wisdom.

12.1.7 The following chronology provided by Ranum (2010) depicts a potted history of where we have come from and implies where we are heading:

1995 - install firewalls;

1996 - punch big holes through them;

1997 - announce "firewalls are dead";

1998 - install intrusion detection systems;

1999 - turn off all the signatures;

2000 - announce "intrusion detection is the pet [sic] rock of computer security";

2001 - install log aggregation systems;

2002 - ignore them;

2003 - complain that intrusion detection still does not work;

2004 - worry about data leaking from the network;

2005–2010 - give employees mobile devices;

2006–2010 - give employees direct-from-desktop Internet publication capability via Facebook, Twitter, etc;

2010 - give employees control of their own IT—when is it all going to sink in? … *On one hand, we're worried about data leakage, and on the other, we take steps to make said leakage as easy as possible.*

12.1.8 In other words, we continue to experience repeated patterns of behaviour and the capacity to run the risk of fulfilling expectation by doing so. Applying technological solutions to technological problems; seeking to develop new technologies to address old technology faults, does little to address the human factors. The risks that consumerisation in the workplace brings will not be halted unless we ensure these issues are embraced within appropriate organisational security policies and procedures in order to deliver effective IA.

12.2 What is IA?

12.2.1 IAAC defined IA as "the certainty that the information within an organisation is reliable, secure and private. IA encompasses both the accuracy of the information and its protection, and includes disciplines such as InfoSec Management, Risk Management and Business Continuity Management. IA is central within any holistic approach to business assurance and should be embedded as an integral part of corporate governance and risk management processes" (IAAC, 2003).

12.2.2 This definition focuses attention on the centrality of information to holistic business assurance. The point is to alter perceptions such that IA comes to be seen not as an "add-on" but as something to be embedded throughout an organisation; the aim must be to develop

12.2.3 Further definitions largely concur:

> "IA is achieved – and must be maintained – through a process that includes the assessment of threats to an information system, an analysis of the vulnerabilities in the system, an understanding of the impact of a system failure, and the application of technical and non-technical countermeasures to reduce the risk to an acceptable level for the business" (US NIST, 2001b).
>
> "IA is a holistic approach towards protecting information and IS by ensuring availability, integrity, authentication, confidentiality and non-repudiation. Although building on the discipline of InfoSec, the concept of IA raises the profile of security as a business critical operational function rather than as a technical support function" (Anhal *et al.*, 2002).
>
> Central government defines IA as "the confidence that IS will protect the information they carry, and will function as they need to, when they need to, under the control of legitimate users." IA should be seen as both a business enabler and a business protector, "ensuring users of IS are not unwittingly exposing themselves to unacceptable risk" (McFadzean, 2005).

12.3 What is IAAC?

12.3.1 IAAC's mission is to advance IA to ensure that the UK's Information Society (InfoSoc) can count on a robust, resilient and secure foundation. It is a private sector-led, not-for-profit forum engaging key stakeholders in public and private sectors.

12.3.2 Its actions include contributions to government policy development; specific briefings to its members, meetings and conferences on relevant issues. IAAC produced the first Manifesto for the UK – "Protecting the Digital Society" in 2002. It addressed all the issues (and more) that are now being repeated in 2016 as concern(s) grow with the interconnectivity arising from IoT.

12.3.3 IAAC was uniquely positioned to lead the debate in the UK on IA at the top of the wave, with the following characteristics:

- *professional,*
- *independent (commercially and politically),*
- *UK focused with international perspective and*
- *multiple stakeholders.*

12.3.4 IAAC has been successful in:

- *addressing the concept of IA with its Manifesto; (then with CSIA and DTI)*
- *inspiring public private collaboration with its paper "Sharing is Protecting"; (then with NISCC, ENISA)*
- *Stimulating public awareness raising with its debate on Cyberhood Watch; (then with ENDURANCE, NISCC)*
- *Informing Decision Makers on IA aspects with the presentation of "DIAN Guidelines" and setting up the Director's IA Network.*

These outputs are crossed referred to in the below Chronology.

12.4 Why IA?

12.4.1 The long term goal is to achieve a good level of IA throughout the Digital Society, for the systems and data that people rely upon in their daily lives to be well behaved. This means:

- *That IS will protect the data they process, store, and communicate;*
- *That they will function as they need to;*
- *That they will function when they need to;*
- *That they will function under control.*

12.4.2 Government has always preferred self-regulation whilst wishing to endorse strong ecommerce as vital for the UK in terms of position and development. However, whilst the private sector have generated multiple solutions, there is insufficient evidence to confirm the success of this approach.

12.4.3 Over the past decade Turnbull, Enron, Corporate Social Reporting, Higgs, the FSA, vendors such as Microsoft, Oracle and IBM have all contributed to increased board awareness of risk management. Then there was the HMRC data breach of 2007 which resulted in the following swathe of reports that highlighted the need for and importance of IA:

- *IPCC independent investigation into the HMRC loss, 61 pages, (IPCC, 2008)*
- *Kieran Poynter Review of InfoSec at HMRC, 109 pages, (Poynter, 2008)*
- *House of Commons Justice Committee Protection of Private Data Report, 28 pages, (UK House of Commons Justice Committee, 2008)*
- *Sir Gus O'Donnell Data Handling Procedures in Government, 46 pages (UK Cabinet Office, 2008b)*
- *Nick Coleman Protecting Government Information - Independent review of government IA, 31 pages, (Coleman, 2007)*
- *House of Commons Home Affairs Committee Report on Surveillance Society, 119 (main report) + 281 (supporting report) pages, (UK House of Commons Home Affairs Committee, 2008)*
- *Sir Edmund Burton, Review into the loss of MoD Personal Data, 76 pages, (Burton, 2008)*
- *MoD Action Plan in response to the Burton Report, 28 pages, (UK MoD, 2008)*
- *House of Commons debate on Data Protection held on 12 June 2008 led by Baroness Miller of Chilthorne Domer, 31 pages, (Miller, 2008)*

- *Ministry of Justice Data Sharing Review, Richard Thomas, the Information Commissioner, and Dr Mark Walport, Director of the Wellcome Trust, (Thomas, 2008)*
- *Review of Criminality Information – Sir Ian Magee (Magee, 2008)*

12.4.4 The benefits and returns from creating a corporate IA culture and corporate IA programmes are expected to include:

- *More assured continuity of business processes and services and of the business itself*
- *Greater efficiency and higher levels of performance of internal operations*
- *Better security, integrity, reliability, and utility of IS and data (higher levels of maintenance of the corporate information infrastructure)*
- *More reliable, and better leveraging of, the goodwill, trading and support relationships established with partners, stakeholders, customers, investors, government and the public.*

12.4.5 The risks of neglecting this aspect of corporate governance might include:

- *Higher operating costs, including both daily costs due to inadequacies of the information infrastructure (e.g. from poor records management) and irregular costs due to major incidents or adverse events*
- *Greater uncertainty in forecasting and planning future costs*
- *More difficult and less beneficial relationships with partners etc*

12.4.6 As stated: "IA must be maintained throughout the life-cycle of a system, as threats change with the changing political or business environment, vulnerabilities appear and disappear as the configuration of the system changes and new weaknesses are discovered, and the impact of systems failure changes as dependency on a system develops" (UK Cabinet Office, 2007a).

12.4.7 Sir Edmund Burton (IAAC chair during the life of this research) highlighted that "the theme of IA had been a continuing challenge for government departments since 2001 (Room, 2009). The following chronological review of developments during the last decade and more, show the maturation during a period of time.

12.4.8 Material in the IA space is being produced weekly if not daily and thus the volume is staggering. The Literature Review is as accurate and up to date as possible up to the date of thesis printing. This is supported by the IA chronology below which traces *some* of the historical events that have impacted the information industry. The flow is intended to be reflective of the growth and maturation of the information industry and IA specifically. Every effort has been taken to refer to the most appropriate and obvious sources. Any glaring omissions are unintentional. The endeavour has been to highlight key points from each publication (where available, directly from their summary details) in order to plot a course through to the present day, focussing on the most seminal, pivotal and influential publications (in whatever format). A number of the works are from a personal collection and, in some cases, are now unable to be sourced online – a reflection of records management in the 21st century. Contact the author for access if unsuccessful.

12.5 IA Chronology

12.5.1 **1440s** – invention of Johannes Gutenberg's printing press.

12.5.2 **1512** – Dutch humanist Desiderius Erasmus in his textbook, *De Copia* stressed the connection between memory and reading, urging students to annotate their books(Carr, 2011, p.178).

12.5.3 **1710** – separation of ownership of information from its production, with the introduction of the Copyright Act.

12.5.4 **1727** – Benjamin Franklin introduced the first public library to Philadelphia, enabling wider access to knowledge sharing.

12.5.5 **1766** – *Freedom of the Press Act* in Sweden

12.5.6 **1775** – Samuel Johnson, in conversation with others regarding the merits of reading is quoted as saying "Knowledge is of two kinds. We know a subject ourselves, or we know where we can find information upon it." (Carr, 2011, p.143).

12.5.7 **1780s** – Jeremy Bentham credited with the design of the *Panopticon* (originally formulated by his brother Samuel) which has often been articulated in the context of the "surveillance society" of the 21st century (McMullan, 2015).

12.5.8 **1789** – *All Writs Act* – which compels people to do things within the limits of the available legislation. Various future rulings diluted its intent though context is king (Lewis, 2016).

12.5.9 **1808** – the first documented "man in the middle" attack. 15th – 24th August 1808 - Lord Cochrane destroys a series of French semaphore stations along the coast of the bay of Marseilles – taking care to copy rather than remove the signal books, leaving the originals to burn amidst the other papers. As a result, the French did not feel it necessary to alter their signals and the British could lie off shore and read those covering the movement of shipping and reports of sightings of the British ships "from the promontory of Italy northward". [Taken from Admiral Lord Cochrane – *The autobiography of a Seaman*. This story is picked up and adapted copied by C S Forester in a Hornblower story and appears again in one of Patrick O'Brian's Jack Aubrey Books).

12.5.10 **1830s** – there was a private sector telegraph covering stock movements in Paris. In 1836, two bankers from Bordeaux bribed telegraph operators to add signals on the price movements of government stocks (sent by post to the provinces) to the network used for official government transmissions. The fraud ran for two years before it was detected, but the trial collapsed because the law on the Government monopoly of traffic was unclear. It was tidied up in 1837 (Flichy, 1993).

12.5.11 **1852** - *Records of Common Council* – regarding records release.

12.5.12 **1861** – the First Battle of Bull Run, also known as "Battle of First Manassas" – the first major battle of the American Civil War, created through misinformation and the art of information warfare.

12.5.13 **1867** – law on electronic signatures clear because of existing legislation – common law liabilities already exist.

12.5.14 **1883** – Augustus Kerckhoffs (Kerckhoffs,1883) stated six design principles for military ciphers, listed below:

1) *The system must be practically, if not mathematically, indecipherable;*
2) *It should not require secrecy, and it should not be a problem if it falls into enemy hands;*
3) *It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;*
4) *It must be applicable to telegraph communications;*
5) *It must be portable, and should not require several persons to handle or operate;*
6) *Lastly, given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its users to know and comply with a long list of rules.*

Modern computing renders much of the content moot, however his second axiom remains critically important and is referred to as Kerckhoffs principle.

12.5.15 **1885** – the public sector purchased its first typewriter, apparently much to the protest of calligraphers in the Civil Service (Shanes, 2011)!

12.5.16 **1919** – GCHQ formed as the Government Code and Cyber School.

12.5.17 **1942** - the UK Government focus was only on the **C** of CIA (Confidentiality)

12.5.18 **1943** – AIIM International was founded as the National Microfilm Association, later becoming the Association for Information and Image Management. In the 21st century, the focus shifted to enterprise content management (ECM) embracing content/document management, business process management, enterprise portals, knowledge management, image management, data warehousing and data mining (Kahn and Blair, 2009). There is no direct reference to security and yet the intrinsic links need to be understood within the information landscape.

12.5.19 **1944** – *Simple Sabotage Field Manual* produced by the Office of Strategic Services (OSS), designed to "assist privy personnel in devising methods that would cause dithering, delay, distress and destruction, from telegraph operators to railway engineers" (Rid, 2013, p.73)

12.5.20 **1945** – Vannevar Bush (1988) wrote an article entitled "As we may think" describing an imaginary information retrieval machine, the Memex.

12.5.21 **1945** – Samuel F.B. Morse introduced the telegraph and people worried about confidentiality of the messages being transmitted so within a year, a commercial encryption code had been developed to protect telegraphed messages. "A few years after that, the US government sought ways to tap into the protected messages" (Garfinkel, 1995, p.118).

12.5.22 **1948** – *A Mathematical Theory of Communication* Available at: http://seclab.cs.ucdavis.edu/projects/history/seminal.html) – Claude Shannon's seminal paper (found on a list of other seminal papers). Provided a mathematical theory for encoding information by applying a value to it – either 0 or 1. From this begat bits and bytes. Shannon is viewed as a founder of information theory and an architect of our digital world.

12.5.23 **Late 1940s** – ***cybernetics*** - concerned with the study of communication and control systems in living beings and machines. The more recent use of the cyber- prefix has been adopted as a result of the more literal meaning "through the use of a computer" (Kingova, 2013).

12.5.24 **1957** – BCS formed.

12.5.25 **1958** – *Public Records Act* - An Act to make new provision with respect to public records and the Public Record Office, and for connected purposes. Updated in 2005 and again in 2011.

12.5.26 **1960s** onwards - cyber temporary or nonce words appear in modern parlance – cyborg being the most memorable.

12.5.27 **1961** – *The economics of information* – Stigler's pioneering article begins thus: "*One should hardly have to tell academicians that information is a valuable resource: knowledge is power. And yet it occupies a slum dwelling in the town of economics"* (Best, 1996, p.22).

12.5.28 **1962** – First formal computing department in Purdue University, Indiana, US.

12.5.29 **1963** – the term "hypertext" was coined by Ted Nelson, implying that each text in systems occupies a position in a multidimensional space.

12.5.30 **1965** – the idea of the "paperless office" was first introduced (Peltier, 2002, p.3). Given where we are in the 21st century, some five decades later, we are far from the "paperless office" and much of the information leaks and data breaches are experienced as a result of the mishandling of information that is left lying around desks and offices – printers, fax machines, photocopiers - rather than being properly managed and controlled.

12.5.31 **1966** – *Cybermen* first appear in the Doctor Who series – The Tenth Planet.

12.5.32 **1966** – *Freedom of Information Act in the US* (under Lyndon Johnson)

12.5.33 **1967** – historical knowledge of software initiatives gaining momentum. First packet switched network developed at the National Physical Laboratory in Middlesex, UK.

12.5.34 **1968** – McLuhan, Fiore and Agel (1968) developed the concept of online hypertext and the global village.

12.5.35 **1968** - computer systems starting to take off – government already taking wrong turns; subsequently written up in books like *Crash* (Collins, T. and Bicknell, D. - 1997) and *Software Runaway* (Glass, R.L. - 1998).

12.5.36 **1969** – saw the launch of the first node of Arpanet in the US, made between two computers in California.

12.5.37 **1970s** – software security assurance work began. TCP/IP protocols agreed, Arpanet progresses to the Internet. The first real email was introduced in 1970.

12.5.38 **1971** – Raymond Tomlinson invented email, choosing the @ symbol to signify location of receivers of messaging, when he launched the service to a US government network. He died in March 2016.

12.5.39 **1972** – File Transfer Protocol (FTP) developed.

12.5.40 **1972** – *Bad Vulnerability Management* – a Computer Security Technology Planning Study, J.P. Anderson – highlighted here only to show how far back vulnerabilities have been being talked about and addressed. There are two volumes available (see the Bibliography). The content addresses the changing landscape of the movement from closed systems (largely internally facing, with a known number of users) to more open systems (with external connectivity and a less predictable user base). The "malicious user in the context of a resource shared system presents a new type of threat, control of which is necessary before the objective of full use of shared computer systems can be realized" (Anderson, 1972, p.10). The summary highlighted the difficulty of having raised issues that required significant control and these having not being met favourably. This has been a constant refrain throughout the intervening years. Maintaining secure systems takes time and costs money. Anderson noted "merely saying a system is secure will not alter the fact that unless the security for a system is designed in at its inception, there are no simple measures to later make it secure" (Anderson, 1972, p.40). Reference monitors, trap doors, penetration testing, file encryption techniques, building secure systems..... the groundwork is evident in these papers.

12.5.41 **1972** – *Cyborg*, novel by Martin Caidin – which inspired *The Six Million Dollar Man* and *The Bionic Woman.*

12.5.42 **1973** - first overseas connection to ARPANET introduced when a connection was established via a satellite link and then land line to University College London and then to Brighton.

12.5.43 **1976** – *Governance* included as part of ISACA discussions and group focus.

12.5.44 **1978** – Bulletin Board Systems (BBS) invented.

12.5.45 **1979/1980** – Usenet invented.

12.5.46 **1980s** – "The early 1980s witnessed a flurry of interest in the application of IM concepts to the harnessing of distributed information and computing resources in the university sector" (Best, 1996, p.144).

12.5.47 **1981** - the Council of Europe Convention established standards among member countries, to ensure the free flow of information among them without infringing personal privacy. The original purpose was to facilitate the flow of data. This is referred to as the Strasbourg Convention of 1981 and was the original data protection law.

12.5.48 **1982** – William Gibson, science fiction writer, coined the phrase "*cyberspace*" in his science fiction novella *Burning Chrome* (Goodell, 1996). Cyberspace is defined as the "notional environment within which electronic communication (esp. via the internet) occurs" (Oxford English Dictionary). Gibson spoke about the use of the term in the 2000 documentary "*No Maps for These Territories"* - "All I knew about the word "cyberspace" when I coined it, was that it seemed like an effective buzzword. It seemed evocative and essentially meaningless. It was suggestive of something, but had no real semantic meaning, even for me, as I saw it emerge on the page".

12.5.49 **1984** - the UK's first Data Protection Act was introduced. This was an act of Parliament designed to protect individuals who have information about them held on computer. The act obliged organisations holding personal data to register with the Data Protection Registrar and agree to abide by the principles of data protection outlined in the act. These principles included: obtaining and processing data fairly; ensuring accuracy and relevance of information; and taking effective measures to prevent unauthorized access to data. Individuals have the right to be told if a third party holds information about them, obtain a record of that information, and require correction if necessary. The 1998 Data Protection Act gave employees the right to see their personnel records.

12.5.50 **1985** – veteran comedian Ernie Wise made Britain's first ever mobile phone call.

12.5.51 **1986** – the CIO – Chief Information Officer was introduced as a role (Best, 1996, p.148).

12.5.52 **1986** – the launch of Fuji's first disposable camera was the biggest technical breakthrough.

12.5.53 **1988** - *The Morris Worm* – introduced new speech acts into the relevant disciplines.

12.5.54 **1989** – '*hacking'* was by now a fashionable media term (Goodell, 1996).

12.5.55 **1989** – Bash was first written (Lucas, 2015, p.4)

12.5.56 **1989** – 10,000 nodes reached on the Arpanet and it becomes clear it is getting larger than anticipated.

12.5.57 **1989** – *ISF* founded - the InfoSec Forum (ISF) is a non-profit company that provides insightful guidance and opinions on a variety of security information. It combines the in-house expertise, experience and collective knowledge of over 300 members across the world to provide easy to use tools and methods that assist its members with a wide range of issues and challenges whether they are compliance driven or strategy related (see for example ISF, 2013).

12.5.58 **1991** – *Computer Ethics Institute* formed and created *The Ten Commandments:*

1) *Thou shalt not interfere with the works and files of other people.*
2) *Thou shalt not sneak around in other people's computer files.*
3) *Thou shalt not use a computer to steal and do negative things.*
4) *Thou shalt not use a computer to bear false witness.*
5) *Thou shalt not copy or use proprietary software for which you have not paid.*
6) *Thou shalt not use other people's computer resources with no authorisation or proper compensation.*
7) *Thou shalt not appropriate other people's intellectual output.*
8) *Thou shalt think about the social consequences of the programme you are writing or the system you are designing.*
9) *Thou shalt not use a computer to harm other people.*
10) *Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.*

[Sic. The confusion of "thou" and "you" is in the original.]

12.5.59 **1991** – *Gulf War* – It is widely believed that the Gulf War was the first information war. "In many ways, the Gulf War was the harbinger of IA. The ability to rapidly integrate commercial and military information technology from multiple companies and countries and the ability to dynamically reconfigure it was critical to the success of the Allies" (Herrmann, 2002).

12.5.60 **1991** – *McCumber's CIA Model* – the CIA triad is borne – confidentiality, integrity, and availability are widely discussed as attributes of security.

12.5.61 **1991** - World Wide Web developed and introduced..... CERN makes WWW freely available, websites and web browsers developed during the 1990s.

12.5.62 **1992** - *Cadbury Report* – defined Corporate Governance as "the system by which organisations are directed and controlled. The Board of directors are responsible for the governance of their organisations". This set the tone for the organisational level of

attention required to the subject area and introduced the term *stakeholder* into our day to day dialogue.

12.5.63 **1992** – 1,000,000 hosts on the internet.

12.5.64 **1992** – *COAST* formed – Computer Operations, Audit and Security Team in Purdue University.

12.5.65 **1992** - *Basel Capital Accord* – this was first published in 1988, replaced again in 1999 with a more comprehensive and risk-sensitive framework to include operational risk areas. It was finally implemented in 2007 and is now on its third iteration. Given the depth of available resources, knowledge and regulation behind risk management thinking in the financial services sector, a lot of which was adopted within the public sector, it is alarming to appreciate the level of the collapse within the banking industry during the latter part of the first decade of the 21st century.

12.5.66 **1992** – 'cypherpunks' – a group of California libertarians – set up an email list to purpose and discuss how cyberspace could be used to guarantee personal liberty, privacy and anonymity.

12.5.67 **26 November 1992** – *Organisation for Economic Co-operation and Development (OECD) Guidelines for the Security of Information Systems* - "These guidelines apply to all participants in the new information society and suggest the need for a greater awareness and understanding of security issues, including the need to develop a "culture of security" - that is, a focus on security in the development of IS and networks, and the adoption of new ways of thinking and behaving when using and interacting within IS and networks. The guidelines constitute a foundation for work towards a culture of security throughout society". This was a theme that was being considered towards the end of the 20th century, being talked about nearly *twenty* years ago and yet it is still a struggle to achieve it in the second decade of the 21st century.

12.5.68 **27 November 1992** – *Amended proposal for a Council Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data.* This 1992 proposal would be further debated and negotiated before enactment as Directive 95/46 (the Directive) – which became the 1998 Data Protection Act in the UK.

12.5.69 **1993** – The term *Critical Information Infrastructure* (CII) originated in the US in 1993. The OECD phrased 'Information Infrastructure' consisting of those information and communication technology facilities, networks, services and assets which, if disrupted or destroyed, either (1) have a serious impact on the health, safety, security or economic well-being of citizens or the effective functions of governments, or (2) causes the functioning of a critical infrastructure which it supports to be seriously disrupted'.

12.5.70 **29 April 1993** - *US House of Representatives Subcommittee of Telecommunications and Finance, first session, Rayburn Office Building* – John Gage, Director of the Science Office at Sun Microsystems gave a hands-on demonstration of how the world was going digital (Goodell, 1996). It served to show the breadth and scale of the potential of digital technology and how easily locatable any individual would become but also how much information would be traceable and accessible as a result of the operation of so many databases.

12.5.71 **May 1994** - *High Risk/High Potential: An Executive Report on the Management of Information Technology in Local Government, Audit Commission* (2014a) "There is a risk that change will outpace the ability of IS to support it. Councils must endeavour to align their IS with changes in their organisation. Knowing where the organisation is going is a necessary starting point." ..... "There must be corporate standards for shared data which must be owned, managed and reconciled with the operational packages that are purchased. Those who use IT need no longer be beholden to IT specialists. They can gain control and shape the council's IT strategy to meet their changing needs and obtain the IT support that they require". This did not start to happen for at least another decade. "Users must become better educated and trained if they are to get the best out of existing systems. Failings are often caused by user error or ignorance rather than any weakness on the part of the provider..... Authorities should underpin their training programmes with a skills audit of their staff." One of the key components of any IA strategy is embedding IRM as a fundamental activity throughout the organisation. "Whilst most Councils acknowledge the need for effective IS, other issues tend to distract attention. ….The management of statutory change has become all-absorbing for councils. There is a risk that managers 'sideline' the development of their council's information strategy."

12.5.72 **May 1994** - *High Risk/High Potential: A Management Handbook on Information Technology in Local Government, Audit Commission* (2014b) - This report was the full detail of the Executive Summary above. It provides an excellent "history" timeline for the growth in usage of ICT in local government. The continual implications were of savings that may be possible for the appropriate deployment of new technologies. However, there was a clear understanding that this would require re-working of Service Level Agreements to reflect the reality of the contractual nature of the activities. There was a reference to the need for "a federal IT Strategy". Given that this review is showing where some of the "cracks" are in terms of the use of terminology, it is likely that anything with the branding of "federal" implies too strong a US link and that this could have unwittingly alienated the intended audience. As one would expect there was acknowledgement that "as the number of users increase, so does the risk" and the recommendation was to provide advice to include "security of data stored on fileservers and personal computers; managing data stored outside the central IT department and

implications of the Data Protection Act". There was a rather prescient point on page 52 – "the causes of failure are rarely technical". On page 73, there was a "call to arms" in the conclusion implying the need for a National Framework for IT – "the government should initiate discussions with the local authority associations to identify the benefits of further national specifications". In March 2011, a new Government ICT Strategy was released.

12.5.73 **June 1994** – NSTISSI No. 4011 – *National Training Standard for Information Systems Security (InfoSec) Professionals* – discussed information states and security measures required to be implemented.

12.5.74 **1995** – *BS7799* – the first British Standard for InfoSec management is issued.

12.5.75 **1995** – 16 million people using the internet worldwide, most of them computer enthusiasts (Lucas, 2015, p.xviii).

12.5.76 **1996** - *(96/938) Keeping it Confidential* booklet from the *DTI (as was)* and companion booklet *"Protecting Business Information – Understanding the Risks"* – "An organisation's information is one of its most important assets. It needs to be protected, particularly since it is often shared within the organisation and with trading partners". The booklet is about classification and protection of information and the provision of assurance of effective management of IP in organisations. Security measures should be justifiable, practical and necessary. Effectively this is a handbook for helping to implement what was the Manual of Protective Security (MPS), without needing to have access to the restricted document. The terminology is addresses business risk, impact, threat, vulnerability... these terms have been used for at least two decades and yet there is still a requirement to either explain them or be apologetic for them.

12.5.77 **1996** - first UK council website was launched.

12.5.78 **1996** – the Internet Watch Foundation (IWF) was founded.

12.5.79 **1996** – saw the first real concerns about investment in IT; reality of IT implementations saw failures to bring proposed benefits. The problem was identified as "confounding information with IT", as articulated by Best (1996, p.21).

12.5.80 **1997** – Nicholas Negroponte – former Director of MIT Media Lab – declared that the internet would bring about world peace, and the end of nationalism.

12.5.81 **1998** - Corporate governance was recognised by the Critical Infrastructure Assurance office (CIAO) who chose to partner with the Institute of Internal Auditors (IIA), the National Association of Corporate Directors, the American Institute of Certified Public Accountants and the IS Audit and Control Association (ISACA) – and hosted a number of summits to raise awareness of the role of

corporate directors in safeguarding the information assets of their organisations.

12.5.82 **1998** – *Moonlight Maze* began but was not discovered for a further two years. This is the code name for a long term infiltration of American defence institutions. Over 17 years later, it is of concern to acknowledge the lack of progress, in technological terms, given that it can still take over 200 days to identify an infiltration in a network.

12.5.83 **1998** - *Parkerian Hexad* – Donn Parker adds possession, utility and authenticity to the existing CIA triad, viewing these as atomic elements.

1998 Highlights and Lowlights

- *The Data Protection Act 1998, which built on an EC directive of 1995 was introduced with the explicit aim of protecting the right to privacy. It embedded the 8 Principles into the process.*
- *CERIAS formed – the Center for Education and Research in Information Assurance and Security, Purdue University.*
- *"We are staking our future on a resource that we have not yet learned to protect", George Tenet, Director of the Central Intelligence Agency (Lucas, 2015, p.1).*

12.5.84 **March 1998** - *Protecting Critical Information Infrastructures Conference and Exhibition* - the first of several run over the subsequent years capturing the flavour of the time period where the subjects elucidated through the publications reflected herein were brought to a wider audience for discussion and dissemination.

12.5.85 During **1998**, Neil Fisher (now Chair of IAAC) was involved in providing talks on IA and its journey from Information Warfare, to the MoD. This provided audiences with the opportunity of the beginning of real learning about the IA concept in the UK.

12.5.86 **December 1998** – *Our competitive future: Building the Knowledge Driven Economy* - This paper set out the Governments ambitious goal of developing the UK as the world's best environment for electronic trading by 2002. Embedding IA was always going to be fundamental to achieving this goal.

1999 Highlights

- *Carnegie Mellon refers to the term survivability.....*
- *Tony Blair made a statement that "all government departments" would be BS7799 certified – this was quickly changed to compliant once the cost implications were clear.*
- *Scott McNealy, cofounder of Sun Microsystems, made the infamous statement "You have zero privacy anyway. Get over it!".*

12.5.87 **1999** – US Department of Justice identified *IA* as a national priority in the US for the protection of the critical information infrastructure.

12.5.88 **5 March 1999** – *Building confidence in Electronic Commerce – A Consultation Document* - A paper designed to consult on the proposed implementation of the government's policy target of achieving 25 per cent of dealings by citizens and businesses with government as electronic by 2002. This was the beginning of the electronic and transformational government agenda, seeking to encourage trust in the use of online systems for government purposes.

12.5.89 **March 1999** - *Cabinet Office Modernising Government White Paper* – advocated that the public sector "use new technology to meet the needs of citizens and businesses and not trail behind technological developments". This was a significant sea change in UK Government ICT positioning at the time and was the birth of "Information Age Government".

12.5.90 **1999** - *National Infrastructure Security Co-ordination Centre (NISCC)* was established with an announcement by the Right Honourable Tom King MP. Resourced by existing Security Service and CESG baselines, it acts as an umbrella organisation co-ordinating relevant activities in several departments and Agencies, including the Security Service, CESG, Cabinet Office, Home Office, MoD, DERA, DTI and the Police. Note the pattern forming that for each US announcement soon after there is a UK equivalent.

12.5.91 **1999** – *ISO15408 The Common Criteria for Information Technology Security Evaluation* (abbreviated as Common Criteria or CC) is released - an international standard (ISO/IEC 15408) for computer security certification.

12.5.92 **1999** – Tim Berners Lee - "I have a dream for the Web [in which computers] become capable of analysing all the data on the Web – the content, links, and transactions between people and computers. A 'Semantic Web', which should make this possible, has yet to emerge, but when it does, the day-to-day mechanisms of trade, bureaucracy and our daily lives will be handled by machines talking to machines" (in Jones and Ashenden, 2005, p.165).

12.5.93 **1999 –** *Sherwood Applied Business Security Architecture* (SABSA, undated) - was used in a major exercise in the US Government as far back as 1999. Australia's Federal Government has seen SABSA use and adoption in a number of agencies.

12.5.94 **May 1999** - the Organisation for Economic cooperation and Development (OECD) endorsed the OECD *Principles of Corporate Governance* which constitutes the chief response by governments to the G-7 Summit Leaders' recognition of corporate governance as an important pillar in the architecture of the new century's global economy. These Principles defined "corporate governance" as "the systems by which business corporations are directed and controlled" [ICGN Statement on Global Corporate Governance Principles – Adopted July 9, 1999 at the Annual Conference in Frankfurt].

12.5.95 **September 1999** - *(Turnbull Report) Internal Control: Guidance for Directors on the Combined Code (ICAEW, 1999)* – required that companies ensure that they have a sound system of internal control and effective risk management processes which the Board reviews regularly, applicable to the "security of tangible and intangible assets, business continuity issues". Turnbull requires companies to ensure their system of internal control is a) embedded in the operations of the company b) is capable of responding to change and c) includes procedures for reporting major weaknesses immediately. The guidance required companies to manage their key risks, remedy weaknesses promptly and review all aspects of internal control on a regular basis.

12.5.96 **19 November 1999** Bruce Schneier wrote the following, which is apposite considering the currency and veracity of the statements (Schneier, 1999):

Predictions

- *As systems get more complex, **security will get worse**.*
- *As systems become more interconnected, **security will get worse**.*
- *Unless manufacturers are held liable for security failures, **security will get worse**.*
- *The only long-term solutions are to either embrace insecurity or eschew "Internet-years" style complexity.*
- *In the short term, the best course of action for enterprises is to outsource security to companies that have the expertise to understand the systems being secured."*

2000 Highlights / Lowlights

- UK Freedom of Information Act.
- UK Regulation of Investigatory Powers Act.
- 93,047,785 hosts on the internet.
- Amazon, Ebay and Yahoo suffered hack attacks in 2000 that led to share price falls. Ebay lost $4.56 billion, Amazon $6.67 and Yahoo lost £17.24 billion.
- Aug 00 Hacker hits 9 .gov.uk (4 LAs); 450 more sites in 5 weeks.
- **This decade includes global public use of the Internet, search engines, Google, dot.com boom and bust, Web 2.0, social media, 1 trillion web pages in 2008.**

12.5.97 **2000** – the era of "*Electronic Government*" (eGov) began. This spawned many prefix laden activities where "electronic" was put in front of numerous initiatives – including e-governance, e-democracy, much in the same way as later in the decade "cyber" was put in front of initiatives (Kesar, 2011). Note that in the transition, the preceding term was "hi tech crime" but "cyber" has adopted the same trajectory as a prefix for many other terms beyond its original intended scope and meaning.

12.5.98 **January 2000** - *Putting IT into Practice: New Technology and the Modernising Agenda (Hellawell, 2000)* - This document was honest from the start. "It's not easy. Nor is it cheap. It's very fast moving and it's no longer optional. Public sector managers and members have exactly the same mountain to scale as their private sector peers – they have to develop an e-business strategy". The terminology has been the same for a full decade. *Key words and phrases:* Business driven, ICT enabled; hybrid managers required; committed leadership necessary; "IT department to come out of the closet"; citizen centred viewpoint. The report contains reference to a case study showing that Knowsley Council had implemented "community digital television" in 2000 and yet Hull City Council were only considering utilising this technology a full ten years later in 2010. It is a good example of how long and slow the process of change is across the public sector – particularly without a centrally driven mandate to insist on certain implementations for the greater good. Knowsley were smart and made the most of government funding available at the time. There was never going to be enough funding to go around what were over 400 councils at the time.

IAAC established, 21 March 2000 - promoting the concept of IA over information security – providing the only forum in the UK in which industry and government could work together to develop policies that would ensure the emergence of a secure and dependable information infrastructure. During the year, IAAC's *e-Security Monitor* provided its' members with an up to date and comprehensive reference source on IA developments worldwide. The Aims of IAAC are stated as follows:

- To provide a forum for networking and information exchange on Information Assurance and Critical Infrastructure Protection policies;
- To conduct and disseminate forward-looking analysis into Information Assurance and Critical Infrastructure Protection policies;
- To enable business, government, law enforcement and citizens to jointly create, and influence the policy development of solutions to the challenges of the Information Society;
- To promote the creation of a safer and better protected Information Society in the United Kingdom and to assist those organisations with intentions similar to thos e of IAAC to foster awareness of, and action on, Information Assurance globally;
- To engage in education and outreach activities either alone or in co-operation with any company, association, public authority, or other body or person for the purpose of promoting the objectives of the Council.

12.5.99 **March 2000** – *eEurope Initiative, European Commission* - owned by the Information Society DG seeking to make the EU the most competitive and dynamic knowledge based economy in the world with improved employment and social cohesion by 2010 (Chissick and Harrington, 2004).

12.5.100 **27 March 2000** – *Protecting the Information Society* – monthly briefing paper produced by IAAC, BP01 (IAAC, 2000a).

12.5.101 **April 2000** – *eGovernment Strategic Framework* - written to fulfil the commitment of the 1999 Modernising Government White Paper. "The *Strategic Framework* was accompanied and followed by numerous other reports aimed at specific components of the electronic government strategy" (Chissick and Harrington, 2004).

12.5.102 **April 2000** – *UK Policy Developments* – monthly briefing paper produced by IAAC – providing updates, BP02 (IAAC, 2000b).

12.5.103 **18 April 2000** - *Defining the Critical National Infrastructure* - workshop hosted by IAAC followed up with a detailed report providing rhetoric and content for senior executives to utilise and learn from in terms of placing the core critical protection themes within their organisations.

12.5.104 **17 May 2000** – *e-Business Risks seminar* held by IAAC at which cyber themes were discussed – cybercrime, cyber-fraud, cyber-shoplifting. So for these themes to be gaining such traction and media attention in late 2010 and early 2011 seemed surprising to the author, given that the issues at their core are not new and many solutions have already been talked through. As an industry, it is important to start to move beyond talking for the sake of talking, mainly to an audience of peers, as it does not seem to be professional enough when we should have progressed well beyond reaction to proactive behaviours (IAAC, 2000c).

12.5.105 **May 2000** – *US Policy Developments* – monthly briefing paper produced by IAAC – providing updates, BP03 (IAAC, 2000d).

12.5.106 **May 2000** – *The European Union's Approach to IA and CIP Policy* – monthly briefing paper produced by IAAC, BP04 (IAAC, 2000e).

12.5.107 **June 2000** - *eGovernment, an international study of online government* (Oakley, 2000) - "Attitudes to privacy, co-operation, technology, equity and to government itself differ enormously between the countries involved. Nevertheless, benchmarking is a hallmark of any serious attempt to change practice in organisations and it is in that spirit that the report is offered". Again, this is a good example of where a concept had been already gaining traction (that of privacy) and yet it took all of the subsequent decade for it become more widely embedded into the vocabulary and thinking of people working in IS related roles. It seems to be the case that despite things in the information age moving incredibly quickly – as predicted in Moore's Law - the actual human is not keeping up at the same pace (Intel, undated).

12.5.108 **June 2000** – *International Organisations and CIP Policy* – monthly briefing paper produced by IAAC, BP05, (IAAC, 2000f).

12.5.109 **June 2000** – *eEurope 2002 Action Plan* endorsed by the Feira European Council. The aim of the Action Plan was to make available:

- *A cheaper, faster, secure internet;*
- *To invest in people and skills in order to meet the next bullet point; and*
- *To stimulate use of the internet by accelerating electronic commerce, promoting electronic access to government services and health services online.*

12.5.110 **June 2000** – *Russian and Chinese Policy Overviews* – monthly briefing paper produced by IAAC, BP06, (IAAC, 2000g).

12.5.111 **July 2000** – *France and German Policy Overviews* – monthly briefing paper produced by IAAC, BP07, (IAAC, 2000h).

12.5.112 **July 2000** – *North European Policy Overviews* – monthly briefing paper produced by IAAC, BP08, (IAAC, 2000i).

12.5.113 **July 2000** – *Executive Summary, COBIT, governance, Control and Audit for Information and Related Technology (*ITGI, 2000) Even in 2000, there was acknowledgement that information travelling through cyberspace without constraints of time, distance and speed leaves us with increasing dependence on information and the systems that deliver the information, increasing vulnerabilities and a wide range of cyber threats. This document was first issued in 1996.

IT Governance is described as providing the structure that links IT processes, IT resources and information to enterprise strategies and objectives. The vocabulary was about the need for management to ensure, through due diligence that IT control objectives are understood and well managed.

12.5.114 **August 2000** – *CIP Policy Developments in Ireland, The Netherlands, Belgium and Switzerland* – monthly briefing paper produced by IAAC, BP09, (IAAC, 2000j).

12.5.115 **September 2000** – *CIP Policy Developments in Italy, Spain, Portugal and Greece* – monthly briefing paper produced by IAAC, BP10, (IAAC, 2000k).

12.5.116 **September 2000** - *UK Online (2000)* – major campaign announced by the then Prime Minister, Tony Blair with the intention for the UK to become the best country in the world for e-commerce. This included a £1bn drive to get all government services online by 2005 and £15m to help businesses make the most of the web.

12.5.117 **October 2000** – *Australian and Canadian Policy Overviews* – monthly briefing paper produced by IAAC, BP11, (IAAC, 2000l).

12.5.118 **2 November 2000** – *Protecting Critical Information Infrastructures, Dr Andrew Rathmell, Chairman, IAAC for Compsec 2000* - In his speech, Dr Rathmell talked about the fact that building the dependable infrastructures upon which the InfoSoc relies posing a bewildering array of new problems to public policy makers and corporate leaders alike. “although there is a growing recognition amongst business of the importance of assuring information assets, many sectors and organisations do not yet recognise that IA is a business critical activity”. (Rathmell, 2000)

12.5.119 **October 2000** – *Pacific Rim Policy Overview* – monthly briefing paper produced by IAAC, BP12 (IAAC, 2000m).

12.5.120 **December 2000** – *Israel, The Arab States and North Africa CIP Policy Overview* – monthly briefing paper produced by IAAC, BP13 (IAAC, 2000n).

12.5.121 **December 2000** – *Risk Analysis – a Review, by the IAAC Dependencies and Risk Working Group (DRWG)* – concluded that although some methods and tools exist for assessing risk at the system and organisation level, none were suitable for assessing risk across dependencies. Also, methods for mapping dependencies need to include political and social elements rather than just technical ones (IAAC, 2000o).

12.5.122 **2000** - *Chance or Choice? Risk Management and Internal Control guidance for Local Government* outlined the need for corporate management teams to drive the commitment to risk management throughout their organisations.

This remains the case and the author continues to see many organisations where there is a disappointing lack of cohesion between IT risks and corporate risks. *(SOLACE, 2000)*

12.5.123 **2000** - *Corporate Governance in the Public Sector– The Role of Risk Management, (Alarm, 2000)* – This paper gave public sector senior managers, elected members, non-elected board members or non-executive directors some practical ideas on how to try and ensure that their organisation has in place the necessary requirements to achieve effective risk management and so contribute to effective corporate governance.

2001 **– Highlights / Lowlights**

- e-everything continued "in anger" – e-government, e-procurement, eEurope, e-Procurement, e-Commission..... supplanting previous *cyber* formations – i.e. e-commerce, not cyber-commerce. During this time, cyber took on the more negative formations- *cyberwar, cyber attack, cybercrime, cyberterrorism and cyberbullying.*
- March 01 'PoisonBox', 'Hi-Tech Hate' groups target .gov.uk, sites including Local Authorities.
- June 01 Alldas.de *(previously attrition.org, then zone-h.org)* lists several UK Local Authority sites defaced.
- July 01 Three Welsh Local Authority sites attacked.
- CESG IA Review.

12.5.124 **2001** - *Risk Management in the Public Sector, CIPFA/ALARM* the point of highlighting these related risk reports is to show that there has long been available guidance on embedding corporate risk management practices that are robust. However, it has not always been the case that the intrinsic links between InfoSec risk management and corporate risk management are as well established (CIPFA, 2001). The guide's coverage includes:

- *What is risk management?*
- *The elements of successful risk management*
- *Embedding risk management within the organisation*
- *Identifying the risks*
- *Assessing the likelihood and impact*
- *Determining the response and agreeing action.*

12.5.125 **January 2001** - *Field Fisher Waterhouse (FFW) "Preparing for e-government seminar*" scheduled for 14 March 2001, letter to all Heads of IT in Local Councils - FFW sent out a pack to all Heads of IT in Local Councils including relevant articles – most of which reflected the key issues that need to be borne in mind in implementing the new systems. The concerns at the time were much more about managing outsourcing contracts and IT procurement.

12.5.126 **January 2001** – *Critical Infrastructure Protection and Crisis Management in Britain* – monthly briefing paper produced by IAAC, BP14 (IAAC, 2001a).

12.5.127 **30 January 2001** - *Ross Anderson, Why InfoSec is Hard – An Economic Perspective* – Anderson (2001) is a key industry figure who has been writing and contributing for many years. This is a seminal paper that highlights how "information insecurity is … due to perverse incentives. Many … of the problems can be explained … clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons."

12.5.128 **2 February 2001** - *Communication from the European Commission to the Council and the European Parliament Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime* - This Communication discussed the need for and possible forms of a comprehensive policy initiative in the context of the broader *InfoSoc* and *Freedom, Security and Justice* objectives for improving the security of information infrastructures and combating cybercrime, in accordance with the commitment of the European Union to respect fundamental human rights. (Commission of the European Communities, 2001) IAAC (and no doubt many others) commented on this in March 2001. It was part of an increasing movement at the time that saw greater involvement from Europe and thus raised the whole subject of InfoSec further up the required agenda.

12.5.129 **February 2001** – *Protecting Online Financial Services through New International and National Supervisory Regulations* – monthly briefing paper produced by IAAC, BP15 (IAAC, 2001b)

12.5.130 **2001** - *National Audit Office survey published* – 82 per cent of central government departments agreed that risk management was important to the achievement of their objectives, but few had risk management objectives and policies. Only 57 per cent of departments had procedures for reporting risks and only a third said that regular risk reports were an effective component of managing risks in their department. Since 2003/2004, all central government bodies have been obliged to publish full Turnbull-style internal control statements, covering both financial and non-financial risks.

By now, there is growing acceptance that, given the value of intangible assets to contemporary businesses, IA is a theme that should be an integral part of corporate governance. Information is fast becoming the most valuable corporate asset, and is essential to the survival of a business. In order to practise IA effectively, information assets within an organisation need to be identified and then valued.

12.5.131 **6 March 2001** – *Enabling Business Through IA, Protecting Critical Information Infrastructures presentation by Dr Andrew Rathmell, Chairman* (IAAC, 2001c) – Rathmell addressed the annual *Protecting the Critical Information Infrastructure* conference, speaking of how e-business and e-government brought tremendous benefits but, at the same time, increased dependence means increased risks. National and international IA required new policies and partnerships (a decade on, in 2011, this is what the same kinds of people are saying about "cyber" security – without appreciating that it is the *same thing*). Rathmell made a clear case for it not being solely a government issue and for it also not being solely a technology issue. Policy, legislation and technology-based capabilities should be developed at the information content and service layers, as distinct from the carriage and transmission infrastructure layers. IAAC had also raised the issue of there being a need to engage with the "digital citizen" and the consumer. This led on to the theme of Cyberhood Watch, akin to Neighbourhood Watch.

12.5.132 **19 March 2001** – *Military Dependency on Civilian Infrastructures* – IAAC briefing paper highlighting that being part of the global 'ambient network' and a global Information Infrastructure presents new challenges, repeating much of the earlier March paper, BP16 (IAAC, 2001d).

12.5.133 **Spring 2001** – IAAC Board and Secretariat members contributed a chapter on InfoSec to an Institute of Directors' Guide to InfoSec – which was released to 52,000 CEOs across the country. IAAC's *Code of Ethics for Computing and Network Usage* was included in the IoD Guide and launched to the public in March 2001.

12.5.134 **April 2001** – IAAC launched *Policy Papers on IA* following a year-long consultation with its members and the government, private sector and academia. These papers covered threat and risk, current and future research and development initiatives and trends, best standards and guidelines for IA and Critical Infrastructure Protection (CIP) and recommendations on conducting a national public education and awareness programme for IA. Some of the latter became embedded in GetSafeOnline.

12.5.135 **3 April 2001** – *The Costs of Cybercrime* - At the time of writing the IAAC BP17, it was stated that "The FBI will not investigate a security incident unless the monetary damage is above US$5000, someone's life was in danger, or interstate commerce was affected". No doubt the intervening time period has moved those goal posts. The

conclusion had some interesting points, including that "the only way for the average internet user to quantify loss will be through direct experience and historical precedent" (IAAC, 2001e).

12.5.136 **April 2001** – *IoD IA Business Security and Trust in the Internet Age*, London - This document only describes IA in terms of the Confidential, Integrity and Availability (CIA) triad of the InfoSec Management System (ISMS) and is quite technologically focussed rather than expressing the breadth of IA as we have seen it to historically actually mean. So this means a generation of directors have been ill informed. In terms of intention, it was ahead of its time but it went backwards in 2005 with an *InfoSec* publication which was actually more of an *IT security* work. It was presumably deemed too difficult to sustain the use of the term IA at director level.

12.5.137 **2001** – *CESG Review* - Government IA work began when CESG went onto a repayment regime for its government work. CESG focussed on project work and there was felt a need to take a more forward look. Therefore Cabinet Secretary Richard Wilson asked Sir Edmund Burton to look at the issue. This was meant to be a narrow look but Burton concluded that there was a much wider set of government and national risks. He recommended the creation of a central sponsor to champion IA across the public sector and to private sector and individuals. The review report identified a need for additional Government funding for IA activities (Room, 2009).

12.5.138 **22 May 2001** – *First Annual Computer Privacy, Policy and Security Institute, Attorney General John Ashcroft* – this speech addressed cybercrime and cyber criminals and could equally be presented in present day, removing reference to connecting to the internet via a modem. Cyber rhetoric was on the agenda and the need to address the risks through improved legislation and understanding by professionals was raised at that time. Yet a decade on there appears to have been less progress than one would imagine was appropriate for the "information age".

12.5.139 **May 2001** – *Technical Security Issues and Trends for Critical Infrastructure Protection* – monthly briefing paper produced by IAAC, BP18 (IAAC, 2001f).

12.5.140 **6 June 2001** – *COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS - Network and InfoSec: Proposal for a European Policy Approach* (European Commission, 2001) - This Communication provided the strategic outline for action in this area. It was considered to be a first step and not a definitive action plan for network security in Europe. However, it already made suggestions for actions in order to establish a framework for a common European approach. The next stage was for the framework and the proposed actions to be discussed by Member States and the European Parliament. The Commission proposed to launch a thorough

discussion with industry, users and data protection authorities on the practical details of implementing the actions proposed.

This is an interesting document as a pivot point of acknowledgement of the change coming from the distinction between the historical closed loop systems to the more open and connected complex systems of the 21st century. The convergence was highlighted as being an area requiring policy and legislation change, particularly in relation to national security. The definition of security requirements for network and IS as described in this paper use the CIA characteristics at the core, *plus* **authentication**.

12.5.141 **8 June 2001** - *Establishing Trust in Cyberspace: Regulation or Self-regulation?* IAAC seminar at CBI Conference Centre, London. The topic was "on the table", albeit from a perception that was pre-9/11 2001, at the time.

12.5.142 **June 2001** – *The Domain Name Systems (DNS) and the Protection of Corporate Identity on the Internet* – monthly briefing paper produced by IAAC, BP19 (IAAC, 2001g).

12.5.143 **June 2001** – *IA Model,* Maconachy *et al.* (2001) – mapping information states to InfoSec needs.

12.5.144 **July 2001** – The *Civil Contingencies Secretariat (CCS)* was set up to co-ordinate government responsibilities for dealing with disasters. It was unable, however, to use its position at the heart of government to lead a strategic response to the new threats post 11 September 2001 (see *Defence of the UK* report below).

12.5.145 **July 2001** – *Worth the Risk, Audit Commission* - The risk management approach to internal control plays a significant part in securing good governance structures. Identifying and dealing appropriately with the key strategic risks facing an authority enables it to identify the key actions it must take to deliver its main goals. This paper was intended to help local government bodies in England and Wales to improve the way in which they identify, evaluate and manage significant risks. The idea was for it to help local government members and officers to assess whether their risk management activities were satisfactory and developing in line with the best value initiative. Included in this management paper:

- *An introduction to risk management and its benefits*
- *Risk management in local government*
- *The role of members*
- *What senior officers can do to implement better risk management*
- *Pitfalls to be aware of.*

12.5.146 **2001** - *Private Security Industry Act* – addresses the question of standards, education, training and regulation of security professionals and providers. The Security Industry Authority was formed following on from this.

12.5.147 **18 July 2001** - *IAAC Y2K Lessons Learnt* - highlighted that the Year 2000 (Y2K) experience left senior managers feeling that "their involvement in IT security was complete.....due to the finite deadline and the fact that no major problems arose". However, the benefits were that it afforded the allocation of funding, gave legitimacy to such a project and established some momentum. "General tendency to see IA and InfoSec as a technical issue to be delegated to the IT section by senior management.

Without management support, it is difficult for an InfoSec Manager to implement effective IA strategies and measures on a company-wide basis. A key message was that operating without full Board support makes it difficult to effectively deal with the different dimensions of IA, such as personnel concerns, awareness, legal considerations, policy concerns. To re-engage senior management, however, it is necessary to demonstrate that IA is essential to the organisation". The language of change (p.34) – sought to promote the concept of IA over that of InfoSec. The US had some success with this tactic, according to Nancy J. Wong of the CIAO. A decade later the same tensions, concerns and internal justifications have arisen, as cyber subsumes IA. Similar challenges arise around digital vs IT and business continuity vs resilience.

12.5.148 **19 July 2001** - *IA and Good Corporate Governance Issues and Options Paper* - seminar held at Institute of Chartered Accountants for England and Wales, London followed by the publication of the paper. Again, linking the issues of IA and Corporate Governance in alignment with the Turnbull report requirements.

12.5.149 **19 July 2001** – *IA and Corporate Governance seminar*, Institute of Chartered Accountants for England and Wales, London – "Underwriters simply do not know what the risks are and therefore have no history of losses by which to set premiums" (Chris Cotterell, Safeonline). Whilst the published outputs implied that IRM had its origins in petrochemicals and then in the insurance industry, it has proven difficult over the last decade to generate sufficient interest and support from the insurance industry as a whole to take on policies that support businesses in insuring themselves against "cyber risks".

12.5.150 **July 2001** – *National R&D Strategy for IA* – Policy Paper prepared by IAAC.

12.5.151 **26 July 2001** - *Establishing Trust in Cyber-Space: Regulation or Self-Regulation* (BP20) (IAAC, 2001h) - This paper examined whether market forces will solve the problem of assuring the UK's critical information infrastructures or whether the state needed to take a more active role. It argued that new, collaborative models of regulation needed to be adopted and that the market could not be left to provide the necessary security. The concern was that the government needed to take a number of steps, including

consideration of additional regulation in relation to security standards and incident reporting.

12.5.152 **September 2001** – *Raising Awareness of IA in the UK* – Policy Paper prepared by IAAC (2001i).

12.5.153 **September 2001** – *A Safety Critical Software Approach to InfoSec* – monthly briefing paper produced by IAAC, BP21 (IAAC, 2001j).

11 September 2001 – *terrorist attack on New York's Twin Towers*

There was a definitive impact on the rhetoric of risk and threat assessment and response and the legislative statutes as a direct result of ***9 September 2001.***

12.5.154 **September 2001** – *Building Partnerships to Protect Europe's Information Infrastructures,* (Rathmell, 2001) - "....failing to maintain an informed view of the level of cyber-threat will soon be an unsustainable risk for board level decision-makers". Again, a decade on in 2011, cyberspace is being discussed as if it were a new and burning topic – and yet the evidence shows that those involved in the discussion have already done so on several previous occasions and in many ways could do worse than revisiting conclusions previously reached and updating these, rather than at the expense of the public purse continuing to hold meetings, conferences, seminars and the like on a subject that has sufficient body of evidence to refer to already. Determinedly having more and more talking shops appears to put off the need to actually move into action mode and yet this is the kind of example that baffles history students year in and year out – when they can see that information was available to people who should have known better than to repeat the mistakes of those that had gone before, if only they had paid attention and got on and done something constructive rather than sitting around and talking about it some more.

12.5.155 **10 October 2001** - *Statement of Eugene H. Spafford, Professor of Computer Science and Director of Purdue University's Center For Education and Research in IA and Security, House of Representatives Science Committee* - Spafford stated that:

> …a myth that is often repeated, namely that industry will find incentives to solve our security problems. To the contrary, it is largely because of industry practices that we currently face such security problems! Industry is concerned with getting products to market as quickly as possible, at the lowest cost. The result is often software with extraneous, poorly designed and poorly tested features. To spend extra time or money on better security is to put the companies at a disadvantage in the marketplace. Instead, many software companies have disclaimed all liability in their licenses, and sought to insulate themselves from adverse reactions and scrutiny of their software… In the current market that does not offer consumers significant choices, and where there is no liability for faulty products, there is little likelihood that industry players will invest in fundamental research to improve products.

Apart from the most obvious security changes that Microsoft made in terms of their Trustworthy Computing platform, there is much truth in what Spafford was saying (Spafford, 2001).

12.5.156 **26 October 2001** – *USA Patriot Act* – The title of the Act is a contrived seven letter acronym (PATRIOT), which in combination stand for *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* of 2001. The Act reduced restrictions on law enforcement agencies' ability to search telephone, e-mail communications, medical, financial, and other records; eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and broadened the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The act also expanded the definition of terrorism to include domestic terrorism. The act was set to expire May 29, 2011. On May 26, 2011 President Barack Obama signed the PATRIOT Sunsets Extension Act of 2011, granting a four year extension of three key provisions – roving wiretaps, searches of business records and conducting surveillance of "lone wolves" (individuals suspected of terrorist-related activities not linked to terrorist groups).

12.5.157 **15 November 2001 - "***Presenting the InfoSec Case to the Board of Directors, Audit and Control***"** (NACD, 2001) – conducted by the National Association of Corporate Directors, the Institute of Internal Auditors and KPMG – only one quarter of the respondents indicated that InfoSec on the board's agenda at least once a year, whilst only one eighth of respondents' boards discuss InfoSec at least quarterly. IAAC recommended that:

> …as Corporate Governance guidelines are rewritten and updated, the role and importance of IA as an integral part of corporate governance process must be clearly articulated, and that IA auditing and reporting requirements should be incorporated into the regular auditing process. …Greater attention should be given to building a business case for IA in business language. The issue of language must also be considered. Senior management needs to hear a business case articulated in business terms if the concept of IA is to be accepted. There is a clear need for improved communication between the Board and the IT Security Department, so that both parties understand their roles and the reporting functions expected of them.

The same statement could be made in 2017, and people would nod wisely, agreeing that something *must* be done, and yet doing nothing.

12.5.158 **16 November 2001** - *Building a Safe and Secure Information Society: UK Public Policy Requirements, IAAC Recommendations* (IAAC, 2001k) - This paper provides IAAC's recommendations for action by the UK Government to promote trust and confidence in the nation's information environment.1 Trust and confidence can be developed by promoting IA. The term IA ensures that the focus is on holistic business assurance; i.e. assurance of information as a

business enabler relevant to the highest levels of management. Government has a central role to play in promoting trust and confidence in on-line activities both by acting as an example of good practice and by virtue of its position as the largest single procurer of goods and services in the UK economy.

Conversely, poor standards of IA in critical and public systems will undermine confidence throughout society and in the private sector. The following actions should be prioritised:

- *Adherence of all public bodies to best IA practice, implementation of ISO17799 as part of a good corporate governance approach;*
- *Encouragement of public sector bodies to take additional steps to promote trust (e.g. trust marks, codes of ethics, user education programmes, comprehensive incident monitoring and reporting);*
- *Audit of government IA performance by independent body (e.g. Parliament; NAO);*
- *Enforcement of minimum IA standards on suppliers to public sector at all levels.*

Existing mechanisms should be used to promote adoption of good IA practice. The following actions should be prioritised:

- *Imposition of mandatory minimum standards compliant with ISO17799;*
- *Promotion of IA-aware culture;*
- *Development of "no-blame" mandatory reporting of InfoSec incidents parallel to existing incident/accident reporting mechanisms.*

It is disappointing reading, when you review all the reports written in 2007/2008, given that all the recommendations were there, available and shared with the right people ahead of significant public sector data breaches, loss of trust and damage to reputation.

12.5.159 **18 November 2001** - *IA and the Public Sector, Neil Fisher, IAAC presentation* – the presentation utilised the themes highlighted in the paper referred to above - *Building a Safe and Secure Information Society: UK Public Policy Requirements.*

19 November 2001 *- Anti-Terrorism, Crime and Security Act* **–** a UK legislative response to the 9 September 2011 terrorist attacks on New York City was introduced, receiving royal assent on 14 December 2001.

12.5.160 **November 2001 –** *Council of Europe Convention on Cybercrime* (ETS, 2001) – this was the Convention that sought to harmonise national legislation across European states – on cybercrime – strengthening and aligning national investigative capabilities, given that cybercrime is a boundary-less activity and great co-operation is required between various agencies. This convention has *still* not been ratified by the UK even though it was represented in March 2010 (UK OPSI, 2010). It was signed by the Council of Europe, more countries than the EU – including Canada, Japan, the United States, and South Africa on 23 November 2001, in Budapest.

As of July 2015, the non–Council of Europe states that have ratified the treaty are Australia, Canada, Dominican Republic, Japan, Mauritius, Panama, Sri Lanka, and the United States.

12.5.161 **November 2001** – *Information Flow in IA* – Policy Paper prepared by IAAC, BP22 (IAAC, 2001l).

12.5.162 **November 2001** – *Information Sharing Review: Sharing is Protecting* – Policy Paper (IAAC, 2001m).

12.5.163 **27 November 2001** - *IA: A different perspective, Neil Fisher, IAAC.* The most significant statement in this report is as follows:

> What 11 Sep 01 has exposed is that the second wave of realisation of the Digital Age is that people are involved within these Digital Environments and they must be identified in a non-repuditable way to allow society to operate in a safe, secure and protected way. The lesson is that People matter hugely and that IA is not just about information and infrastructure issues but about (digital) life itself.

12.5.164 **December 2001** – *IA and Good Corporate Governance* – Policy Paper prepared by IAAC, BP23 (IAAC, 2001n).

12.5.165 **15 January 2002 -** IAAC hosted a Roundtable to help solidify the work towards IAAC's White Paper "*IA and Corporate Governance: Engaging Senior Management*". The intention was to identify priority areas that require further work and to agree actions that can be taken forward in terms of linking IA and corporate governance. By emphasising IA, the intention was to promote security to the highest levels in corporate leadership and to link IRM into business assurance at the top level. IAAC's working groups also identified on a number of themes:

- *Standards working group – acknowledged BS7799 provides good practice;*
- *Dependencies and Risk Working Group – identified that a 3 Tier Model – upper, middle and lower organisational approaches – was required; suggesting tools and techniques. The outputs eventually became the DIAN Guides – Directors IA Network Guides;*
- *Information Sharing Group linked their activities to CPNI, WARPs and the eAware agenda.*

The rhetoric was starting to consider measurement and metrics, measuring trust, security and benchmarking IA but provided an acknowledgement that IA is not always a quantifiable entity. The identified positive and negative incentives for 2002 were:

- *Negative incentives include damage to reputation and avoidance of legal liability both for entity and individual directors*
- *Positive incentives include competitive advantage (through using IA as a marketing differentiator), lower costs as a result of reduced insurance premiums, impact on shareholder value and corporate social responsibility (CSR).*

There was an emphasis on the need for a strong audit function: "There is a need for the audit community in the UK to better acquaint itself with the new risk environment and the processes that need to be implemented in order to manage it, so that it can accurately report to the Board on the effectiveness of controls."

2002 – Highlights / Lowlights

- ***US Sarbanes-Oxley Act*** Introduced to restore investor confidence after the collapse of Enron.
- Engineering discipline cross over starting to be seen – safe and reliable software required.
- IAAC embraces holistic definition for IA and works with Government on NIAS.
- Feb 02 Regional Local Authority suffers Syn Flood attack on Server then Router.
- July 02 SQL Injection vulnerability in several Local Authority sites.
- August 02 Local Council DoS attack using similar MAC addresses – printers unavailable.
- eEnvoy appointed as Central Sponsor for IA.
- CSIA Secretariat set up (by 2010, this became known as the Information Security and Assurance [IS&A]) – a unit within the UK Government's Cabinet Office.
- eGovernment Strategy Framework Policy and Guidelines for Security issued.

12.5.166 **15 January 2002** – Microsoft, through Bill Gates – launched the Trustworthy Computing Initiative (TCI) (Microsoft, 2002). Gates' called upon employees across the company to fundamentally rethink their approach to product development and strive to deliver products that are "as available, reliable and secure as standard services such as electricity, water services and telephony." (Source no longer available)

12.5.167 **February 2002** – *Identity Theft Highlights the Importance of 'Data Responsibility'* – Policy Paper prepared by IAAC, BP24 (IAAC, 2002a).

12.5.168 **February 2002** – the acronym GRC was borne from a realisation of the growing importance of the combination of services relating to Governance, Risk, and Compliance being delivered by Forrester (Rasmussen, 2015).

12.5.169 **March 2002** – *US Critical Infrastructure Protection Policies since 11th September* – Policy Paper prepared by IAAC, BP25 (IAAC, 2002b).

12.5.170 **19 March 2002** - *Bob Evans, OeE Presentation - Resilience: From Potential to Actual* - Quoted Sir Richard Wilson, Head of the Civil Service as saying "IA is right in the centre of the playing field… In a networked world, threats can arise and spread far more quickly than we are used to… It is important for government to have its own house in order". The rhetoric has always been there but the resultant expected follow through does not appear to be evident, perhaps, hence the volume of repeated reporting. There were several core themes to this presentation:

- *Core business process must include IA risk assessment e.g. ISO 17799;*
- *You get what you pay for: do you know what you paid for?*
- *The need to cover the end to end security threat, both physical and electronic;*
- *The need for HR involvement and supporting internal policies.*

12.5.171 **2002** - *DTLR e-gov@local, Towards a national strategy for local e-government* - Overall the report identified a number of possible local government services that could be provided through electronic means. This document can be seen as a "where it all began" paper in terms of e-Government and the later Transformational Agenda. It identified Privacy and Data Sharing requirements would need to be addressed through the development and delivery of Standards, which were due to be available in Spring 2002.

12.5.172 **2002** - *Audit Commission - Councils and e-Government, Research so far* (Audit Commission, 2002). This report included the comment: "The real driver is about customer focus, not about ICT. It's about a new relationship between the council and the customer". The research showed that Council officers cited a lack of ICT skills and knowledge among staff and difficulties with engaging senior officers and members among the key barriers to success. Original research conducted by MORI in 2001.

12.5.173 **April 2002** – *Proposal for a COUNCIL FRAMEWORK DECISION on attacks against IS* Brussels, 19.04.2002, COM(2002) 173 final, 2002/0086 (CNS) (Commission of the European Communities, 2002) - Member States were supposed to bring into force the measures necessary to comply with this Framework Decision by 31 December 2003. So there was clear identification of the need to secure against expected electronic attack in the future.

12.5.174 **April 2002** – *DTI InfoSec Breaches Survey* (UK DTI, 2002) – identified that a "root cause" of the low investment in IA "appears to be that security is treated as an overhead rather than an investment. Business people find it difficult to apply normal commercial disciplines to IT security. ….. It is also the case that most IT security professionals have a technical rather than commercial background, and so may lack the skills in the development of commercial business cases". This document set a dangerous precedent of implying that a commercial business case is what is actually required, when many of the other renowned publications concur that embedding good IA is not about embarking on a project with a start, middle and end, but about changing the culture throughout the organisation so that IA becomes knitted into the fabric of everything that is done rather than being viewed as a project that has a fixed ending.

12.5.175 **2002 -** *Cabinet Office - Privacy and Data Sharing: The Way Forward for Public Services, Performance and Innovation Unit.* This document referenced Public Service Trust Charters – which are Information Charters, a notion which reappeared in 2010 as if they were a new idea. This document, referred to as the "PIU Report" encouraged the implementation of an analytical framework for privacy and ideas for improving and auditing data quality. The important point to note is that any references to "privacy" in a UK context, refer to Data Protection as "the concept of privacy as such is not recognised under English law" (Chissick and Harrington, 2004).

12.5.176 **April 2002** - *Is Britain on Course for 2005, The third KPMG Consulting e-government survey,* (first published in Spring 2000) (KPMG, 2002). The e-government agenda was about ensuring that the entire population could access the service provided by their government and council in a way that they found convenient and comfortable. The case was for coherent multi-channel approaches to public service – integrating these with traditional channels rather than replacing them. This is worthy of note particularly as there will be many citizens who feel that they are being forced down an "all things online" route rather than have traditional channels still being made available to them. However, there are of course cost implications to this which are not always considered.

12.5.177 **April 2002** – *Will Broadband Rollout undermine InfoSec?* – Policy Paper prepared by IAAC, BP26 (IAAC, 2002c).

12.5.178 **16 May 2002 –** saw the launch by *IAAC* of *Protecting the Digital Society: A Manifesto for the UK* (written February 2002) (IAAC, 2002d). This was an important document that set forth a three pronged workshop agenda covering the following initiatives at the time:

1. *Public Policy;*
2. *Corporate Governance and Information Risk Management (IRM, in 2010, resurfaced as an acronym and phrase of note);*
3. *Information Sharing and Awareness.*

The document states that "IA is complementary to top-down risk-based management and audit approaches". The manifesto linked IA to Corporate Social Responsibility (CSR) and being inclusive of data protection (DP), privacy, protection of one's "logical neighbours" and measures to promote ethical use of new technology in the InfoSoc. "IA is as much a part of Corporate Social Responsibility (CSR) as are environmental or human practices so IA is likely to move onto the CSR agenda before too long."

This significant piece of work in the IAAC portfolio called for a "comprehensive national UK strategy":

> the creation of a comprehensive national strategy to ensure that the UK's InfoSoc can count on a robust, resilient and secure foundation. … As the topic of IA is perceived to be boring and technical, the extensive coverage it receives in times of crisis gives a distorted picture to the public.

One of IAAC's key roles has been to assist "HMG in ensuring that messages are co-ordinated, integrated and focused".

IAAC committed to reporting every December, benchmarking the UK's performance in trust and security. The intention was to provide innovative analysis, regularly reviewing how the UK was progressing towards building a secure electronic environment and contrast the UK with examples of good practice from around the world. Whilst the regularity of the reporting fell by the wayside, this particular piece of

research re-introduced the opportunity to survey the IAAC membership in late 2010.

The work that was undertaken included:

- *Examining available approaches and tools in various sectors;*
- *Identifying best and current IA practices/capabilities;*
- *Providing good practice guidance based on real-world cases, noting sectoral variations and identifying gaps and requirements for better practices.*

"Economics of Trust and Security" appeared as a theme. At the time, there was no systematic measurement of how government policy can actually boost trust and confidence and how policy instruments can improve security in the complex, adaptive systems that constitute the globalised information infrastructure. To improve policy making, there needed to be a systematic evaluation of the economics of InfoSec, the costs and benefits of various policy options and case study work on the impact of particular interventions. Corporate governance standards were encouraging companies and public sector bodies to adopt good practices in risk management, including management of information risk. The concern was that security management standards were not widely enough adopted and needed to be complemented by management and audit mechanisms that could give Boards the assurance they currently lack.

The concept of Resiliency was raised within the strategy and was adopted by Central Government prioritizing business continuity more broadly in the public sector, progressing towards the introduction of the Civil Contingencies Act in 2004.

The manifesto articulated that the information infrastructures upon which the wider "information environment" is being built are neither safe nor secure enough to act as a trusted basis for the digital society. Increasing dependence on IS at a time of growing systemic vulnerabilities and threats threatened to undermine confidence in the InfoSoc and poses risks of broader societal disruption.

> The Blair Government is committed to ambitious targets for the digitisation of government and for making the UK a leader in the global information economy. In order to avoid the crisis of confidence that has recently manifested in some of the UK's physical infrastructure, the InfoSoc must be built on secure and robust foundations. Today, however, the information infrastructures that underpin the information environment are vulnerable to attack by criminals, terrorist and foreign adversaries. As we have moved to a society in which instant electronic access to all government and many financial services is expected, disruption of the information infrastructures could effectively bring society to a halt. Yet, lack of trust in the internet as a medium for secure transactions is a key factor in preventing business and citizens going on-line; this not only derails the Government's visions but also sets back the UK's economic growth and international competitiveness.

The manifesto also reflected that market forces alone would not ensure a sufficient level of trust and confidence in information networks. Public policy, it was felt, needed to lead and shape the IA environment to ensure the InfoSoc is built on robust, resilient and

secure foundations whilst business freedoms and civil liberties are protected. Public policy to date had been a mix of a "hands-off" and self-regulatory pro-business approach combined with periodic "heavy-handed" interventions in the name of public security and safety. In general, there had been too little government lead and government intervention but in some cases government intervention has been overzealous and ill conceived. Nonetheless, partly by coincidence and partly by design, the UK state was coming to take more of a lead through a range of regulatory and legislative instruments. The time was therefore ripe for a systematic re-evaluation of UK public policy.

12.5.179 **22 May 2002** - *CYBER HOOD WATCH: Empowering the Digital Citizen, Dr Andrew Rathmell, CEO, IAAC, InfoSec in the Public Sector, presentation* (IAAC, 2002e) - The idea was that Cyberhood Watch would mirror Neighbourhood Watch – which protects individual homeowners against burglary and petty theft, vandalism, low level crimes - but for the online environment, where it is important that people are protected against identity theft, industrial espionage, masquerading etc.

12.5.180 **22 May 2002** - *Making UK Online Succeed, InfoSec in the Public Sector, presentation by Neil Fisher, Vice Chairman, IAAC* - The intentions at the time were:

- *To make the UK the best and safest environment in the world for e-commerce;*
- *To ensure that everyone who wants it has access to the Internet by 2005; and*
- *To make all Government services available electronically by 2005.*

12.5.181 **May 2002** – *Dealing with Cybercrime* – Policy Paper prepared by IAAC, BP27 (IAAC, 2002f).

12.5.182 **May 2002** - *Engaging the Board: Corporate Governance and Information Risk, Aarti Anhal, Stephanie Daman, Kevin O'Brien and Andrew Rathmell* (IAAC, 2002g) – "The single most important finding [of a survey of IAAC members] is that, *even amongst companies with a commitment to IA, there is little agreement on concepts and terminology or on methods for assessing benefits.* Nonetheless, there is a consensus that existing best practices and standards for managing and hence benchmarking IA strategies are inadequate. … To achieve success in this information economy, enterprise governance and IT governance can no longer be considered separate and distinct disciplines" (ITGI, 2002). Risk Management involves the following steps:

- *Identifying the risk*
- *Identifying the consequences of failing to manage risks effectively*
- *Mitigating the risk*

"dependency risk" entered into the domain of thinking and articulation – and was built upon to develop resilience strategies etc.

This report also acknowledged that "IA costs money". It is not a saving: ... "In general, companies will do the minimum required in

order to comply with negative incentives. To go beyond this, an organisation needs to see real business benefits in doing so".

The report referenced the *2001 CBI Cybercrime Survey* which highlighted that "loss of reputation, through adverse publicity and loss of trust, is a greater fear than financial loss for most organisations" (Mark Grossman, Liability for you if you've been hacked {August 2000}, cited in IAAC, 2002g)

> IA has its own social aspects such as data protection, privacy and the concept of being a good citizen and neighbour, as IA can easily be compromised by someone else's poor practices – the chain is only as strong as its weakest link.

The holistic nature of IA was emphasised by ISACA which described the sister concept of IT Governance in the following terms:

> In the information economy, successful enterprises integrate information technology (IT) business strategies, culture and ethics in order to attain business objectives, optimise information value and capitalize on technologies. Extended enterprises, which incorporate customers, business partners, vendors, stakeholders and constituents, rely on the efficient and effective sharing of information, including goals/expectations, status and ultimately knowledge. Making this at all mission critical to most enterprises … and making it happen as it should happen requires IT governance (ITGI, 2002).

Y2k demonstrated that IA is essentially a management issue requiring executive attention, rather than a technical issue. The DTI's *InfoSec Breaches Survey* 2002 stated that "People have traditionally associated InfoSec with technology and administrative processes. Effective InfoSec is just as much about educating and managing staff, managing incidents to avoid reputation damage, and providing business partners with assurance about security." (UK DTI 2002)

Formed in October 2002 in the Cabinet Office to support Andrew Pinder in his role as Central Sponsor, Dr Steve Marsh became Director of the CSIA. The unit's mission was to provide assurance to government that the risks to the UK national information infrastructure are appropriately managed. It was realised that this was broader than an OeE agenda item, including defence and national security issues. CSIA was made a separate cabinet office unit reporting to Sir David Omand. In 2010, the CSIA became known as the InfoSec and Assurance (IS&A) unit and thereafter the Office of Cyber Security and IA (OCSIA).

This was another solid, influential document produced by IAAC, providing many of the foundations of what have subsequently been embedded as best practice building blocks for IA across the public and private sectors. Key phrases include:

> Corporate Governance now calls for effective management of risks but board-level awareness is not yet being translated into effective controls. … Assurance of a company's information assets is critical to realisation of stakeholder value and of business potential in an economy that increasingly relies on information technology and business transactions using the Internet. However, there is still

> a tendency to under value the importance of IA and to ignore the benefits that can be gained from improved security and providing more information and reassurance for users.

There was an interesting attempt at mapping IA onto BS7799 – "BS 7799 is a comprehensive work of reference and is intended to facilitate the identification of a wide range of IA controls….The Code contains a detailed set of controls that will satisfy the IA requirements of most IT environments across all functional domains." (p.17)

Historically, in the UK, IT audit has been a feature of the Institute of Internal Auditors qualification programme since the early 1980s so there has been oversight of IT activities for a considerable period of time and a great deal of learning about what has worked and what has not across a great many IT projects can be gleaned from audit reports across the land, particularly in the public sector. Yet this report highlighted that there was concern at the lack of available data upon which to base computer security risk-management decisions, believing that too much of it was anecdotal and not representative of any specific industry or group (Hoo, 2000, p.19).

The report concluded thus, "It is through ensuring that good IA standards and practices encompass small companies as well as large organisations that an overall governance framework will emerge that is no longer a "recommended framework" but an "obligatory" one. The standards will not have been mandated by Government, but will come about because industry and government see their value and expect compliance with them as the "normal practice" for business (Hoo, 2000, p.20). The belief at the time was that "There may come a time when regulation is necessary but it would be far preferable to achieve the same result by a combination of soft regulation and a market-based approach.

Such approaches are less likely to become "box ticking" exercises; if boards can be motivated to act of their own accord, then the substance rather than the form of IRM will be adopted."

This is interesting to reflect on in 2011, given other rhetoric that implied, at the time, that allowing "the market" to decide, would not achieve the required cultural shift to embedding IA in a meaningful way, which appears to have actually been the case, given the ongoing slew of breaches and need for both technological, people and process controls to be in place in order to manage and maintain an information infrastructure effectively.

Security and risk are often presented to Boards through the tried and tested approach of "Fear, Uncertainty and Doubt" (FUD). Well governed companies have been seen to perform better over time, thereby increasing share value. Businesses with effective governance plans manage risk better and rebound from setbacks more quickly. IA will become an increasingly important element of corporate social responsibility (CSR).

As with environmental pollution, the security of the networks upon which society increasingly relies is a common responsibility.

This report references a lack of actuarial data which has been a significant factor in restraining the development of a mature insurance market. The reports' author believed that organisations that employ risk mitigation measures and also have in place the right measures to obtain IT specific insurance, stand a greater change of obtaining a lower insurance premiums. Saving money provides a powerful incentive for senior managers to comply with (IA requirements).

12.5.183 **May 2002** - *InfoSec Consultancy A Study for The DTI Prepared by Chris Sundt Independent Security Consultant* (Sundt, 2002) - This Report was commissioned by the DTI to look at existing and emerging issues affecting the confidence users may have in the supply of InfoSec services. This was occasioned by the public debate surrounding the issue of whether the implementation of the Private Security Industries Act should encompass InfoSec consultants. The report addressed the entire range of InfoSec services. It found that InfoSec skills are part of a broader picture. The commonly held view that InfoSec specialists were simply computer security experts underestimated the increasing complexity and importance of modern IS. It was emphasised that InfoSec was essential to many business models and had to be seen as an integral part of the risk management process.

12.5.184 **June 2002** – *NHS Information Governance Toolkit* first launched (UK NHS, 2015). It is described as follows: "The Information Governance Toolkit is a Department of Health (DH) Policy delivery vehicle that the Health and Social Care Information Centre (HSCIC) is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in a single standard as a set of information governance requirements.

The organisations in scope of this are required to carry out self-assessments of their compliance against the IG requirements".

12.5.185 **25 June 2002** *Business Software Alliance (2002) - Government at Risk for Major Cyber Attack in Next 12 Months, IT Pros Say* Again, reference to the fact that almost a decade ago, cyber-attacks were under discussion and solutions were being found.

12.5.186 **June 2002** – *Do IT Security Consultants need a Licence?* – IAAC, BP28, (IAAC, 2002h).

12.5.187 **July 2002** - *In the service of democracy, a consultation paper on a policy for electronic democracy* (OeE, 2002a) - e-Democracy was described as being about using new technology to energise the democratic and political life of the nation. This document attempted to clarify some of the issues and propose a policy that responded to the opportunities and challenges that e-democracy was likely to bring. Security and privacy issues were raised within the document.

This was sent to all Local Government Councils in September 2002 via the Local Government Association (LGA).

12.5.188 **July 2002** – *Company Law Post Enron – Interim Report to the Secretary of State for Trade and Industry and the Chancellor of the Exchequer*, from the Co-ordinating Group on Audit and Accounting (CGAA, p.11) Issues. This report set out the progress to date of the work of the CGAA.

> The Group was set up to oversee and co-ordinate the response in the UK to the issues raised in the aftermath of the collapse of Enron and other corporate failures, and to ensure that UK systems of financial reporting and audit regulation are reviewed thoroughly by the appropriate regulators with the aim of making clear that they are effective and continue to provide appropriate underpinning for strong and efficient national and international capital markets. This report fulfils the Group's commitment to provide a progress report to the Secretary of State for Trade and Industry and the Chancellor of the Exchequer by the summer of 2002.

12.5.189 **15 July 2002** – *Should OFCOM regulate InfoSec?* – monthly briefing paper produced by IAAC, BP29 (IAAC, 2002i).

12.5.190 **15 July 2002** - *Open Source Software use within UK Government, Version 1* (UK OeE, 2002b) - A position paper written at the time. A Google search can easily provide reference to a great many stories relating to the UK Government improving its speed and commitment to open source technologies in 2009, 2010 and 2011 – so this continues to be a challenge for the public sector, balancing the economic gains to be found from the use of open source software, with the increased need to manage perceived data privacy and information-based risk issues.

12.5.191 **24 July 2002** – *House of Commons Defence Committee, Defence and Security in the UK, Sixth Report of Session 2001-02, HC518-1, The Stationary Office, London* - This was quite a significant "after the event" review report. It stated that "As time passes and memories of even such terrible events as the attacks of 11 September begin to fade, the urgency of the priority given to issues of defence and security may diminish. There is an increasing temptation to impose a conventional or historic template on the response to a radical new threat." (paragraph 283) This detailed and sweeping review concluded that the MPs were "disappointed both by the lack of imagination and radicalism in looking for new solutions to match the new threat and by the lack of strategic co-ordination and direction provided by central government". (UK House of Commons Defence Committee, 2002)

12.5.192 **August 2002** – *Digital Identities* – monthly briefing paper produced by IAAC, BP30, (IAAC, 2002j).

12.5.193 **September 2002** – *Dealing with Cyber-terrorism* – monthly briefing paper produced by IAAC, BP31, (IAAC, 2002j).

12.5.194 **September 2002** – *Data Quality included in the NHSIA framework* - Concerns over data quality have consistently been an issue with regard to embedding InfoSec of information assets. This report highlighted some of the key elements to be considered.

12.5.195 **September 2002** – *e-Government Strategy Framework Policy and Guidelines, Version 4.0 (UK OeE, 2002c)* - This document set out a framework for the expression of security requirements for the procurement and acceptance of e-Government services and their implementation. It also described the approach to assuring the presence and proper operation of the security countermeasures put in place to meet the security requirements. This framework document and others derived from it were intended to be implementation independent expressions of security requirements. Implementation constraints were limited to only those necessary to meet government security requirements. Suppliers were free to propose differing implementations constrained only by any interoperability requirements that may be necessary for operational reasons. This framework document did not identify specific services as it was intended to apply to the provision of services in general. Annex C presented a set of example scenarios that illustrated many of the security issues to be addressed. The list was not intended to be complete and would be added to and amended as experience with electronic service provision develops. The security requirements expressed in the framework document represented a call for general alignment with best e-commerce practice, to which government believed it must itself conform. The document, as issued at the time, addressed only functional security requirements and those non-functional aspects of the implementation that permit the services to be readily assured. Assurance, it stated, would also be needed to ensure the presence and proper operation of those functions.

12.5.196 **September 2002** – *eGovernment Strategy Framework Policy and Guidelines, Business Services, Version 2.*0 (OeE, 2002d and Cabinet Office, 2002a) - This document built on the e-Government security policy that set out the e-Government security requirements. It specifically addressed those security requirements related to the provision of business services to support access to e-Government services. The e-Government registration and authentication, confidentiality and trust services framework documents are concerned with proper access of clients and government users to e-Government services, confidentiality of private information involved in transactions and the ability to make binding commitments electronically.

12.5.197 **September 2002** – *eGovernment Strategy Framework Policy and Guidelines, Confidentiality, Version 3.0, OeE, (2002e) Cabinet Office (2002a)* - This document addressed a category of electronic information not previously covered in government security guidance. It complemented existing Cabinet Office guidance on safeguarding

'protectively marked' information (RESTRICTED, CONFIDENTIAL, *etc*) provided by the Manual of Protective Security (MPS). It was anticipated that individual instances of private data handled by e-Government systems would not normally warrant a protective marking. However, there was appreciation that there existed a potential overlap between level 3 confidentiality and material given a RESTRICTED protective marking (see section 3.5.1). In those cases where a protective marking is required, e-Government service providers and implementers could be provided with appropriate guidance from MPS. The case where this was felt to be most likely was in protecting major aggregations of private e-Government information. The detail of this was considered to be beyond the scope of the framework but, for indicative purposes, it was expected that such aggregations would normally warrant a RESTRICTED protective marking. It was considered that guidance from the MPS would always take precedence over that arising from the confidentiality framework. This framework could also have been applied to protection of ancillary information generated as a consequence of electronic service provision, for example, system management information and information on the performance and uptake of e-Government services. Information not covered by the MPS was to be handled in line with this framework. It was noted that the physical and procedural security aspects are important elements of a multi-layer approach to the protection of private information but these were not covered by this framework. Service providers were expected to consider these aspects as part of the overall process for ensuring and maintaining confidentiality. Information marked as PRIVATE should, at government departmental discretion, be handled as RESTRICTED when in a government domain operating under MPS, but should not require baseline security measures. By and large, confusing rhetoric that reads almost like a tongue twister. Given that the extension of central government secure networks rolled out to the local government platform through the implementation of the Government Secure Extranet (GCSx) programme some years later, there was a lot that needed clarification in order to ensure a smooth transition of working practices to a wider audience. Perhaps this is the kind of area where the gap in translation lead to confusion and inertia, thus data based mishap and loss.

12.5.198 **September 2002** - *e-Government Strategy Framework Policy and Guidelines, Network Defence, Version 2.0 (UK OeE, 2002f)* - The essential difference between the business services and network defence frameworks was that the business services framework dealt with protection of the systems and services against failure not prompted by attack (for example against compromise of service through faulty software) and the network defence framework was concerned with protection against malicious and inadvertent attack. If the framework had been implemented and adhered to then there would have been little need for the huge volume of guidance and

reporting that has flowed since. This document introduced the concept of the PRIVATE marking and then promptly said to handle it the same as RESTRICTED – which was the beginning of years' worth of wider confusion across the public sector with regard to protective marking of information assets, in line with previous commentary.

12.5.199 **September 2002** - *e-Government Strategy Framework Policy and Guidelines, Registration and Authentication, Version 3.0 (UK OeE, 2002g)* - This document was concerned with the registration and authentication of citizens and organisations seeking to access government services electronically. It applied in circumstances where government needed to have trust in the identity (real-world or otherwise) and authority of those it was dealing with to ensure that there was no breach of privacy or confidentiality, theft/misuse of data, or other harm. The framework included those cases where anonymous or pseudonymous access was considered to be acceptable.

12.5.200 **September 2002 -** *e-Government Strategy, Security Architecture, Version 2.0 September 2002 (UK OeE, 2002h)* - This security architecture was developed as part of the government's commitment, in the Modernising Government white paper, to developing a corporate IT strategy for government. It was prepared by the OeE, part of the Cabinet Office, on behalf of the e-Champions. The security architecture was seen as an evolving document that would be re-issued from time to time in line with changes in security framework policy and guidelines, implementation experience for UK-Online services and market developments.

This document was aimed at those procuring and providing e-Government services, including Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompassed regulatory bodies responsible for the proper audit and control of public assets and information. In addition it included the suppliers and service providers seeking to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services.

12.5.201 **September 2002** - *e-Government Strategy Policy Framework and Guidelines, Trust Services, Version 3.0 (UK OeE, 2002g)* - This document was intended to set out a number of levels of confidence in trust services used to support e-Government transactions. It was to be read in conjunction with the Security Framework document. The policy was intended only to cover commitments made between clients and government in the context of e-Government services. This included communications between access and back office systems that are necessary to provide an end-to-end service. It did not apply to government-to government transactions that were not concerned with e-Government service provision. It was considered

acceptable to require a client to install a standard commercial security product in order to access e-Government services, for example a web browser with an up-to-date version of the Secure Sockets Layer (SSL) protocol. However, the requirement of client-installed custom software to access e-Government services was to be avoided.

12.5.202 **September 2002** – *eGovernment Strategy Framework Policy and Guidelines, Assurance, Version 2.0, (OeE, 2002h; Cabinet Office (2002b)* - This document was aimed at those establishing, procuring and providing e-Government services. This included Central Government Departments, non-departmental public sector bodies, Local Authorities and other local government bodies charged with the provision of e-Government services. It also encompassed regulatory bodies responsible for the proper audit and control of public assets and information. It included the suppliers and service providers who wished to offer services themselves, provide and operate such systems on behalf of government or provide equipment in support of e-Government services. It was also relevant to security authorities that could have used the document to assess the suitability of offered solutions and accredit them for operational use. The intention was that central government departments and agencies must comply with the framework when installing and operating electronic business services. They were to:

a. ensure that a security concept is developed as part of service concept development;
b. ensure a security policy exists (preferably compliant with BS7799 [as was, ISO 27001 is now]);
c. ensure that a threat and vulnerability analysis to their systems has been conducted;
d. ensure a risk assessment to their systems has been conducted;
e. ensure that the system has been designed, implemented and tested to minimise the risks with appropriately assured countermeasures, both technical and non-technical;
f. ensure that systems are operated in a secure manner, including:
    - *ensuring that processes are in place to receive and act upon current security alerts, warnings and briefings (e.g. use of UNIRAS by a government department);*
    - *ensuring that any patches and updates are tested and implemented in a timely fashion;*
    - *ensuring that threat and vulnerability assessments and hence risk assessment are reviewed on a periodic basis;*
    - *ensuring that compliance with this framework is reviewed on a periodic basis.*

It was **strongly recommended** that other public sector bodies adopt the recommendations of this framework in respect of transactions that they conduct with businesses and the public or which are conducted on their behalf. Where the provision of e-Government services was to be provided commercially, by a third party, the

procuring body was to consider mandating compliance with this framework as part of the contract.

The Security Framework uses the internationally recognised Common (evaluation) Criteria (CC) Protection Profile (PP) model to define the information technology security environment, objectives and requirements for a secure information technology service or product (Chissick and Harrington, 2004).

For protectively marked information or where there is an enhanced integrity and availability requirement the assurance requirements are determined by using HMG InfoSec Standard No.1 (IS1). HMG InfoSec Standard No.3 (IS3) defines the functionality needed to provide assured connections between business domains. IS1 is not currently applicable to material that is not protectively marked, (i.e. most data within the e-Government domain), however, it can be used for integrity and availability. IS3 can be used to recommend functionality requirements for the integrity and availability of business domain connections. In the e-Government domain for each level of service needed (OS1 – OS13) for authentication, trust, confidentiality and network defence there will be an associated set of functionality and assurance requirements.

The Assurance Framework specifically addressed how business sponsors, service providers and developers should ensure that e-Government services are designed, configured and operated in a secure manner. It built on the approach set out in the Security Framework document and detailed a methodology for assessing whether the threats and vulnerabilities to e-Government security systems have been met by appropriately assured countermeasures for each security objective. However, this still placed “Assurance” squarely in the IT domain.

There is a requirement for an “Assurance Framework” which addresses the ways in which trust in the implementation of security elements can be assured. Part of establishing assurance is documenting the security policy, design and operation. This aids the security review process, leading to accreditation. The key components listed above assume the following suggested documentation set:

a) security concept;
b) security policy;
c) security design;
d) security operating procedures.

The Requirements for Secure Delivery of Online Public Services (RSDOPS) made available in 2010 is so similar it is hard to understand why it was necessary or justified to spend tax payers money and time in re-writing what was already available just because it had not been fully adopted (CESG, 2010d). Also, the ongoing struggle to implement a workable protective marking scheme across the wider public sector continues to hamper successful

implementation of best practice due to misunderstandings with regard to how high a level to protect information. The solutions are borne in addressing human factors with regard to balancing an individual's perceived impression of how vital, important or critical all of the information they handle or exchange on a day to day basis actually is when risk assessed against a workable model.

12.5.203 **September 2002** - *Local Government Information Unit (LGiU) - The abc of e-government* The "threat to privacy" is highlighted particularly with regard to "the sharing of data" and the threats posed by the "increasing use of partnerships with the private sector for the delivery of public services". ... "The boundaries between information held in the public and private sectors are likely to become increasingly blurred. This raises the dangerous possibility of the misuse of data by the private sector for purposes of commercial gain". The document concluded that "The type of society that is created in the course of the electronic revolution and the extent to which citizens benefit from digital technology depends very much on the political choices that are made today. Councils have an important role to play in influencing these choices and shaping the future" (UK LGiU, 2002).

12.5.204 **October 2002** – *How can you embed IA in the Board Risk Agenda?* – monthly briefing paper produced by IAAC, BP32, (IAAC, 2002l).

12.5.205 **October 2002** – *"IA and Corporate Governance: What Every Director Must Know"* **–** Jonathan Armstrong, Mark Rhys-Jones and Andrew Rathmell, Eversheds and RANDEurope. This report pulled together the above themes as previously articulated. "One of the key assets for any business is the information it holds. In today's fast moving and competitive world, it is inconceivable that such a valuable asset will not be stored, retrieved and manipulated through the use of information technology. The necessity to preserve and exploit a company's assets therefore requires directors to ensure that they effectively manage their information assets". Director's existing duties – a fiduciary duty to act and exercise powers in good faith and in the best interests of the company; to exercise such skill and care as may reasonably be expected of the role and to carry out the duties imposed by statute.

"Failure to embrace new technology can quickly result in a business falling behind its rivals. The trick is to adopt a strategic approach to IA that will ensure a company benefits from its investments in IT whilst sensibly managing the risk".

12.5.206 **October 2002** – *Engaging the Board: Benchmarking IA (in association with Microsoft)* InfoSec and IT Security are the most common descriptions for this portion of the corporate risk profile. The benchmarking implied that the term IA was becoming more widely used. However, the reality appeared to be that whilst the elements were being increasingly adopted, the term itself had a relatively low usage. IA issues were rarely raised to board of director

level. IA has to be measured to be worthwhile – on the principle that what can be measured can be managed.

12.5.207 **October 2002** – *A Roadmap For Action – Insuring Digital Risk – John Ridd and Rand Europe for IAAC (2002m)* This report identified that Directors and officers have a duty to ensure that their companies carry adequate insurance – yet such insurance does not appear to be readily available. The contention was that stakeholders in businesses and enterprises whose operations include a digital risk needed to recognise:

- *That they have a digital risk;*
- *That their digital risk is not covered by existing general policies;*
- *That even specialist e-business and cyber policies do not cover all digital risks and most do not cover business interruption;*
- *That they need to bring IT properly into the risk management process and integrate IT with business processes; and*
- *That they must work with their insurers and technology suppliers to ensure effective insurance cover as required by their corporate governance and fiduciary duties.*

12.5.208 **November 2002** - *Office of the Deputy Prime Minister, The national strategy for local e-government, www.localegov.gov.uk* - This was a customer access strategy; aimed at re-designing administrative processes to make employees' jobs easier, more productive and more effective. Consultation took place initially through DTLR and LGA. The Strategy referenced from the outset the need to get the consent of the citizens concerned in order to use their data legally. "That consent will not be given if people do not trust government to keep personal information secure and to use it properly".

12.5.209 **November 2002** – *Risk: Improving government's capability to handle risk and uncertainty, Summary Report, Cabinet Office, Strategy Unit* Forward by the Prime Minister – "In many ways life today is far less risky than in the past. Yet risk seems to matter more than ever, partly because we are so much more aware of the risks we face, and partly because of the sheer speed of change in science and technology". Risk handling should be supported by best practice, guidance and skills development – organised around a risk "standard"; setting a culture which supports well-judged risk taking and innovation. Risk management has been found wanting in many recent policy failures and crises. Examples include policies that have proceeded without a full assessment of their vulnerability to events, and major change projects, for example in IT, which have gone ahead without contingency plans. These were highlighted "in the PAC report *Improving the Delivery of Government IT Projects.* Inquiries such as those by Lords Phillips (BSE) and Cullen (Ladbroke Grove rail crash) also make recommendations for improving the handling of risk and communications with the public. While a number of these failures have been down to poor risk management, others raise concerns that public trust has been lost by a failure to be open about the nature of the risk".

12.5.210 **December 2002** – *Promoting a Culture of InfoSec in Europe* – monthly briefing paper produced by IAAC, BP34 (IAAC, 2002n).

12.5.211 **December 2002 –** *Microsoft* launched their *Trustworthy Computing* agenda embracing four pillars – 1) Security, 2) Privacy, 3) Reliability and 4) Business Integrity.

2003* – *Highlights / Lowlights

- **8 April 2003** Report of London Borough website defaced.
- **16 June 2003** *Cabinet Office Draft Civil Contingencies Bill.*
- *EU Reuse of Public Sector Information Directive.*
- *The National Archives (TNA) was formed.*
- During 2003, IAAC members contributed to the Foresight Cyber Trust and Crime Prevention programme.
- CESG releases the National IA Strategy (NIAS) with the CSIA.

12.5.212 **January 2003** – *HMG's Minimum Requirements for the Verification of the Identity of Organisations, e-Government Strategy Framework Policy and Guidelines, Version 2.0, OeE, Cabinet Office (HMG, 2003b)* HMG's minimum requirements for the verification of the identity of organisations was one of a series of documents developed as part of the Government's commitment, in the Modernising Government White Paper, to develop a corporate IT strategy for Government. It was prepared by the OeE, part of the Cabinet Office, on behalf of the e-Champions. It was a clear and concise document that set out the framework as required to be followed.

12.5.213 **January 2003** – *HMG's Minimum Requirements for the Verification of the Identity of Individuals, e-Government Strategy Framework Policy and Guidelines, Version 2.0 , OeE, Cabinet Office (UK HMG, 2003c)* HMG's minimum requirements for the verification of identity of individuals is as per the preceding reference. It has been prepared by the OeE, part of the Cabinet Office, on behalf of the e-Champions. This document built on the e-government security policy and the e-government authentication framework policy. It specifically addressed the Government's minimum requirements for the verification and validation of the identity of an individual.

12.5.214 **January 2003** – *Insurance and Information Risk Management* – monthly briefing paper produced by IAAC, BP35 (IAAC, 2003a).

12.5.215 **February 2003** – *Deterring Cyber-crime* – monthly briefing paper produced by IAAC, BP36 (IAAC, 2003b).

12.5.216 **February 2003** – *Establishing the European Network and InfoSec Agency (ENISA)* Consultation preceding the actual formation in July 2004.

12.5.217 **February 2003** – *The National Strategy to Secure Cyberspace*, (US DHS, 2003) – signed off the Whitehouse, the first Cyber Security Strategy. The UK followed six years later. The Czech Republic issued theirs in 2011. (Czech Republic, 2011).

12.5.218 **15 March 2003** – *Building in Security* – monthly briefing paper produced by IAAC, BP37 (IAAC, 2003c).

12.5.219 **17 March 2003** – IAAC hosted a workshop/seminar for the UK Telecommunications sector and used the following definition (which was then used for other work throughout the year):

> IA is a management process, the purpose of which is to ensure that the critical information within an organisation and the systems and networks that manage it are reliable, secure and private, and that measures and processes are in place to counter malicious electronic based attacks. IA encompasses other disciplines such as InfoSec management, risk management and business continuity management. IA goes beyond Business as Usual InfoSec as it is particularly concerned with high-end threats to systems that are critical not only to the enterprise but also to the wider national or international information infrastructure (Rathmell, 2003*).*

This was the beginning of what became the UK Government's IA Maturity Model (IAMM). An important feature of this definition is that it focuses upon services that are more likely to face extreme risks (e.g. nation state or terrorist attack). InfoSec, in the main, was still only considered to be in the early years of maturing towards IA so the definition was provided to add perspective. However, the part it has to play in protection and governance was better understood and appreciated as a result of many instances of e-crime that had been reported in the preceding few years. A key part of the model and the differentiator was that IA was clearly set as being not just about technical issues. The model was abstracted from six different methodologies e.g. OECD Corporate Governance Guidelines, COSO/Treadway Commission, Turnbull.

12.5.220 ***20 April 2003*** *- Promoting Information and Network Security awareness Among Citizens: A Global Report and Lessons Learned, Aarti Anhal, Shawna Gibson, Lorenzo Valeri (*Anhal, Gibson and Valeri, 2003). This report provided an examination of the existing InfoSec awareness-raising and educational initiatives worldwide targeted at citizens aimed at promoting trust and confidence in the use of ICT. "Much work remains to be done ...before one can truly state that all citizens are sufficiently aware of the risks, rights and responsibilities pertaining to their safe use of ICT".

12.5.221 **April 2003** – *Cyber Terrorism: An Emerging Threat* – monthly briefing paper produced by IAAC, BP38 (IAAC, 2003d).

12.5.222 **April 2003** – *Reform of the Computer Misuse Act (CMA) 1990*, (Internet Crime Forum, 2003) - the Legal Subgroup review took place addressing the changing backdrop of criminal activities taking place in the internet domain. Proposed amendments to the CMA were provided.

12.5.223 **2003** – *IT Governance: A Manager's Guide to Data Security and ISO27001/ISO27002* T- his text book was first published in 2003 and the authors (Calder and Watkins, 2008) defined IT Governance as "the framework for the leadership, organisational structures and business processes, standards and compliance to these standards, which ensure that the organisation's IS support and enable the achievement of its strategies and objectives".

12.5.224 **May 2003** - *e-gov the local e-government standards body, The National Standards Authority for Local e-Government* - Both the agency and the documents appear to no longer exist electronically. However, they set about to embrace security and data standards within a framework. Given how much subsequent work has been done to achieve this, time and effort appears to have been wasted rather than using that which has already been made available.

12.5.225 **May 2003** – *The Insider Threat: The Enemy Within* – monthly briefing paper produced by IAAC, BP39 (IAAC, 2003e).

12.5.226 **May 2003** – *A United Kingdom Government Strategy for IA, Draft Version 0.3 issued by the CSIA* - This strategy set forward a number of critical actions that needed to be undertaken:

- *Appointment of a Senior Responsible Officer for pan-government systems;*
- *Development of the Gateway Process to include IA;*
- *Production of annual information audit statements by departments;*
- *Develop a Common Good requirements process;*
- *Develop and fund an IA Technical Capability Strategy;*
- *Security professionalism for IT staff;*
- *Review and maintenance of communications provision;*
- *Training for Chief Information Officers (or equivalent) and Senior Responsible Officers;*
- *Maintenance and development of pan-government infrastructures; and*
- *Co-ordination of government response to international IA initiatives.*

The business case was claimed not to be clear or available at the time. The Strategy acknowledged that "IA is essential for the delivery of those government outcomes that are dependent on realising the benefits of ICT" (p.14). The Strategy set out with an overarching top down approach but ended up being delivered by bottom up tasks like CESG Claims Tested Mark and the Tiger Scheme. Departments were required by the Cabinet Secretary to ensure that their key systems were compliant with BS7799 (the InfoSec management standard) by 2003 and that all systems should be compliant by 2005 (p.35). There is a lack of evidence in government reporting to prove that this work was achieved satisfactorily.**14 May 2003** – *Proposal for a Regulation of the European Parliament and of the Council establishing the European Network and InfoSec Agency* – held by The Working Party on Telecommunications and Information Society Services of the Council of the European Union. Detailed the scope and objectives of ENISA.

12.5.227 **23 May 2003 –** the *Directors IA Network (DIAN)* met for its inaugural meeting with the aim to:

- *Raise awareness of IA amongst UK corporate boards;*
- *Help produce aware and educated personnel who can contribute to IA in the UK;*
- *Steer practical work from the IAAC and others that will assist boards in meeting their IA duties;*
- *Provide UK Government with advice from industry specialists.*

An IA Framework was created as represented in Figure 92 below:

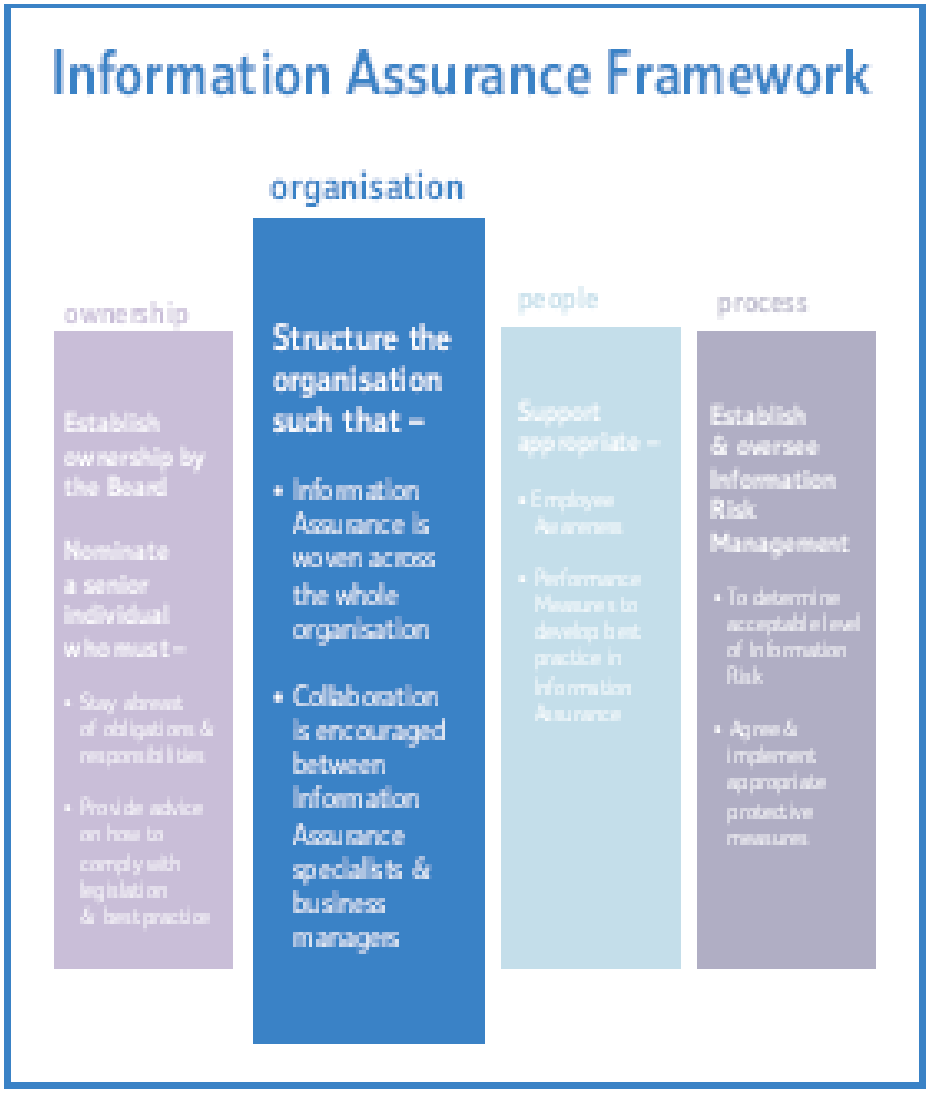


Figure 92: DIAN IA Framework, Source: IAAC (2003m)

12.5.228 **4 June 2003** – Intellect (The Technology Trade Association) launched the *eAware* programme in the UK, based on a European initiative. Report issued in September.

12.5.229 **4 June 2003** – the *CSIA* role was explained to IAAC (UK CESG 2010g) – "to provide assurance to government that the risks to the national information infrastructure are appropriately managed". CSIA defined IA as the confidence that IS:

- *Will function when they need to;*
- *Will function as they need to;*
- *Will be controlled by legitimate users;*
- *Will protect the information they handle; and*
- *Are under the control of the legitimate user.*

So the CSIA was providing strategic direction for government IA activity, sponsoring 'common good' developments; supporting the accreditation of pan-government systems and supporting resilience of government and national ICT. IA was seen as a 'golden thread' that should run through many government initiatives such as:

- *Continuity of government and its service*
- *Defence Strategy*
- *National Counter-terrorist Strategy*
- *National Resilience Strategy*
- *e-Economy and e-Government Strategies*
- *National Crime Strategy*
- *NHS IT Strategy*
- *CJS IT Strategy and so on....*

To provide coherence and support for these initiatives what was being sought at the time was central strategic support to:

- *Ensure that government has a core risk management capability, to support public sector IA; and*
- *Ensure that government influences and benefit from IA activity in the wider environment that is not directly under its control*

The kind of activities that were planned to be supported were:

- *Improving understanding and dissemination of threats, vulnerabilities and impacts*
- *Ensuring the availability of appropriately skilled staff*
- *Developing and maintaining a technical capability, from provision of high grade security to a wide commercial supply of base security products*
- *Ensuring that the public sector 'culture of security' develops to address new risks*
- *Leveraging government procurement to support IA aims*
- *Promoting wider awareness of, and education in, IA*
- *Influencing international activity through, for example, standards bodies.*

The CSIA Director at the time observed "why do you need compliance if it is obviously the right thing to do?" (Marsh, 2003) Indeed, if only that was the case as the future showed from that point onwards.

For context, there were over 450 Local Government Councils at the time and now there are 375. Trust was already a key concern and requisite component. It was accepted thinking that security is a process that had to be engaged in.

12.5.230 **June 2003** – *Reacting to Cyber-crime* – monthly briefing paper produced by IAAC, BP40 (IAAC, 2003f).

12.5.231 **June 2003** - *Policing the Information Society – A Way Forward, EURIM paper* - This is particularly interesting to revisit given that most of the content was re-presented during 2010, further evidencing the author's contention that little has changed in the intervening passage of time. It appears that the same people have attended the same meetings and talked about the same topics to each other at length with little or no discernible change.

12.5.232 **2003** – *IA Guidelines for Boards and Senior Management* - Internal audit was by now recognised as an essential element within a corporate governance framework. The document advised that to deal with IA, an auditor should focus particularly on the specific risks relating to the creation, processing and storage of information and the control and security of the hardware, software and processing infrastructure that form the IS.

The Guidelines covered:

- *Audit;*
- *Risk Management;*
- *Implementation;*
- *Culture;*
- *Support;*
- *Legal perspective;*
- *Planning (Scenario Gaming); and*
- *Return on Investment.*

The report recommended that information on IA incidents should be recorded. It was considered that having available information regarding data found to be inaccurate or incomplete, security breaches, identified hacking attempts, virus or other 'malware' (malicious software) attacks, would aid the assessment of whether any additional measures should be taken to address risks. The report noted that quantitative data – including statistics, recovery time-scales, and the impact and costs of IA compromises – would provide important input into an assessment of the costs and benefits of introducing additional controls to mitigate those risks or improve the processes of recovery.

To deploy risk management successfully within an organisation, it was believed necessary to embed an awareness and understanding of risks and ways to manage them while conducting business as usual. Employees of an organisation should be aware of their responsibility to manage risk in their sphere of influence. This could range from simply ensuring that one's actions do not adversely affect

the safety or security of others – a responsibility on all employees – to strategic board level accountability for IA in general. The starting point was for the Board to own, and be seen to own, the main strategic business risks facing the organisation. By demonstrating ownership, the Board members act as role models for the behaviour of all managers and other employees.

Referenced within the guidance are other resources including *The Association of Insurance Risk Managers (AIRMIC) Guide to Integrated Risk Management* (AIRMIC, 2002) which sets out a road map for any organisation to integrate risk management within business as usual (see www.airmic.com). Also *HM Treasury Orange Book – "Management of Risk – A Strategic Overview with supplementary guidance for smaller bodies"* (UK HM Treasury, 2004), which follows on from other detailed risk management documents already existing in central government, aiming to provide guidance on how to develop a strategic framework for the organisation consideration of risk. It also provides advice on tools and techniques that may be adopted by an organisation to support its risk management processes across the whole range of risks.

Information owners should exist in all disciplines – including HR, IT, Finance, Operations and Strategy – as they play a pivotal part in the successful implementation of IA. On top of these roles, the key to the successful implementation of IA is the coordination of IA with other disciplines such as Risk Management, InfoSec and Audit. It is important that everyone involved in IA implementation understand his or her role. Consideration should be given to providing briefing and training to ensure that there are no misunderstandings.

IA measures fall under three general headings:

1. *Protect and Prevent*; protection of Information Assets
2. *Detect*; detecting incidents – not everyone is obvious and the greatest risk occurs when an incident goes undetected
3. *React and Recover;* log and monitor incidents and events.

An IA culture is built on:

- *Values and principles*
- *The Body of Knowledge (policies, standards, procedures)*
- *Setting attitudes and influencing behaviour (including staff training)*
- *Making the IA aspects of tasks easy rather than difficult*
- *Monitoring, measuring and feedback to encourage approved behaviour*

The guidance included a **Checklist for creating a strong IA culture**

1. Is the Board clear as to the company's IA values and principles, and how are these communicated to staff?
2. When were IA policies last reviewed, and are they consistent with current values and principles?
3. Does management behaviour demonstrate the important attached to IA or contradict it?
4. Do IS reflect the company's IA values, principles and priorities?

5. Is feedback given to staff on the IA aspects of their decisions and behaviour?
6. Do IA procedures or constraints get in the company's way, and if so how has this been resolved?

Key messages included the following:

- To be effective, those responsible for defining policy and conducting risk assessments have to be separated from those who deliver the solutions.
- Following the relevant legislation and guidance in relation to IA will result in positive benefits for any company. This can be considered Good Practice.
- An effective approach to IA does not just make good business sense, it is also a matter of law and Directors ignore the subject at their risk.

So in the breadth of this report can be found sufficient foundations to build an IA framework for any organisation.

12.5.233 **2003** – The *National Archives (TNA) was formed* (Ficenec, 2011) - Born out of the combination of several government organisations; the Public Record Office, the Historical Manuscripts Commission, the OPSI and HMSO, UK Government's official archive contains 1,000 years of history from the Doomsday Book to the present day – and it was where a lot of "old" versions of government department websites were transferred to when the new coalition government came into power in May 2010 and started making expansive changes across the central government information landscape.

12.5.234 **July 2003** – *Information sharing: A 'no brainer' approach to Improved Risk Management* – monthly briefing paper produced by IAAC, BP41 (IAAC, 2003g).

12.5.235 **August 2003** – *Measuring the Benefits of InfoSec* – monthly briefing paper produced by IAAC, BP42 (IAAC, 2003h).

12.5.236 **August 2003** – *Protecting Critical Infrastructures Against Cyber-Attack,* Adelphi Volume 43, Issue 359 (Lukasik *et al*, (2003) - This paper provided a review of some significant study done into the cyber preparedness of various countries. It highlighted the need for more skills and training in the subject area, something that was finally properly picked up in the UK Cyber Security Strategy published in November 2011 (originally launched in 2009). The paper also highlighted a dearth of in-depth research in IA expressing a concern that time was of the essence, but given the paper was written (at the time of writing) almost a decade previously, IA research has not caught up or delivered into the perceived space. The paper also gave a good account of the UK Government's Information Age programme, putting it all together in one place as an overview of the elements that made up the strategy (p.67).

12.5.237 **September 2003** – *Who is responsible for investigating e-Crime?* – monthly briefing paper produced by IAAC, BP43, (IAAC, 2003i).

12.5.238 **September 2003** – *Raising Citizen Awareness of InfoSec: A Practical Guide*, a report by RAND Europe for the eAware project (Wooding, Anhal and Valeri, 2003).

12.5.239 **October 2003 –** *Sharing is Protecting: A review of Information Sharing* – a report produced in association with IAAC and the National Infrastructure Security Co-ordination Centre (NISCC).

12.5.240 **October 2003** – *Awareness Raising in Europe* – monthly briefing paper produced by IAAC, BP44, (IAAC, 2003j).

12.5.241 **November 2003** – *Understanding Trust* – monthly briefing paper produced by IAAC, BP45, (IAAC, 2003k).

12.5.242 **11 November 2003** - *An Engineering Approach to the Design of Accurate and Reliable Security Systems, Dr John Leach* (Leach, 2003) - an article on Threat Based Security Engineering (TBSE), which was deemed to be necessary to help re-frame the thinking, at the time, with regard to the "threat" aspect of the Threats, Vulnerability, Risks conundrum.

12.5.243 **December 2003** – *The Draft Civil Contingencies Bill* – monthly briefing paper produced by IAAC, BP46, (IAAC, 2003l).

12.5.244 **December 2003** - *Office of the Deputy Prime Minister One Year On, The national strategy for local e-government* www.localegov.gov.uk Whilst the progress was deemed to be good, at that point, "the average Council" wanted for "government to develop data protection, authentication/security and common solutions to reduce costs, uncertainty and implementation time".

12.5.245 **2003** - *"delivering service improvement through addressing", The National Land and Property Gazetteer* (I&DeA, 2003). This report referenced the need for improved data quality and analysis which has been an ongoing theme for many years within the industry – and continues to be of paramount importance to the triad element of data integrity that is at the foundations of IA.

2004 – Highlights / Lowlights

Government Spending Review.

The UK ***CIVIL CONTINGENCIES ACT 2004*** was enacted, advising all organisations to maintain plans for the purpose of ensuring, so far as is reasonably practicable, that if an emergency occurs the person or body is able to continue to perform his or its functions.

International focus on detection of IEDs.....but consideration by security personnel of the impact of the social and psychological aspects of this threat vector started to spill into other areas of the "theatre of security".

12.5.246 **17 January 2004** – IAAC reviewed the *IA Strategy* from Government (draft issued April 2003) reiterating previously available advice and guidance.

12.5.247 **9 February 2004** – Sir Andrew Turnbull wrote to all Permanent Secretaries to make clear "the importance of IRM as a crucial component of the board level governance function". This "call to arms" included the advice that:

- *The management of information risk is a Board level function;*
- *They should nominate a Board member to take ownership of information risk – e.g. appointment of Senior Information Risk Owner (SIRO); and*
- *The head of e-government was to work through a board level group of SIROs to ensure the development of culture and processes for effective IRM and for measuring and auditing of performance. Given this was the "call to arms", it is in stark contrast to the kind of statements are lined up alongside the reporting done post the HMRC breach which identified a significant lack of the appropriate leadership or embedded culture.*

12.5.248 **16 February 2004** – *Deception in Computer Networked Defence* – monthly briefing paper produced by IAAC, BP47, (IAAC, 2004a).

12.5.249 **16 March 2004** – *Assured International Passenger Name Record Data* - monthly briefing paper produced by IAAC, BP48, (IAAC, 2004b).

12.5.250 **2 April 2004** – *Cabinet Office IA Stakeholder letter* – introducing the document entitled "*Protecting our Information Systems: Working in Partnership for a Secure and Reliable UK Information Infrastructure*" (UK Cabinet Office, 2004a) and calling for participation and support. The key message was that trust and confidence in IS is essential to ensure uptake of online services. There was a restatement of the fact that "it's not just a matter for the IT department" nor is it "all about firewalls". This is an easy to read document in plain English.

12.5.251 **16 April 2004** – *InfoSec and the Ordinary User* - monthly briefing paper produced by IAAC, BP49 (IAAC, 2004c).

12.5.252 **16 April 2004** – *Reform of the Computer Misuse Act 1990* - monthly briefing paper produced by IAAC, BP50 (IAAC, 2004d).

12.5.253 **April 2004** – *Cyber Trust and Crime Prevention Foresight Project* This UK Government Foresight Project set out to explore the application and implications of next generation information technologies in areas such as identity and authenticity, surveillance, system robustness, security and IA and the basis for effective interaction and trust between people and machines. The Author was involved in this project and the research and thought at the time were in keeping with awareness of the available legislature. The findings have been proven out so far. The Internet of Things was forecast as was the inability to address security from the outset (UK HMG 2003a; Backhouse *et al.*, 2003 and UK Government Office for Science, 2009).

12.5.254 **8 June 2004** - *IA Delphi Questionnaire* (Birchall *et al.,* 2004) research undertaken by Prof David W Birchall and Prof Jean-Noel Ezingeard – in conjunction with the Henley Management College colleagues. The authors wrote about the continued difficulties in articulating IA and gaining board level understanding and acceptance, as evidenced in the responses to their research questionnaires.

12.5.255 **16 May 2004** – *Meeting public sector IA requirements* - monthly briefing paper produced by IAAC, BP51 (IAAC, 2004e).

12.5.256 **May 2004** – *Achieving information* assurance, Research strategy project. Achieving *information assurance is a journey* (Nanton, 2004). It referenced the IAAC National R&D Strategy for IA – "Our current strategy for addressing IA in the acquisition process is the greatest Achilles Heel". Achieving IA begins with a senior level management commitment (typically at the Chief Information Officer level) based on a clear understanding of the perceived threat.

12.5.257 **May 2004** – *Technology Risk Checklist* (The World Bank, 2004) – included cross mapping to the thirteen layers of e-security covering both hardware and software network infrastructures. The rhetoric included reference to "cyber risk mitigation processes" across a comprehensive checklist that preceded the SANS Top 20.

- *Risk Management*
- *Policy Management*
- *Cyber Intelligence*
- *Access Controls / Authentication*
- *Firewalls*
- *Active content filtering*
- *Intrusion Detection System (IDS)*
- *Virus scanners*
- *Encryption*
- *Vulnerability testing*
- *Systems administration*
- *Incident response plan (IRP)*
- *Wireless security*

12.5.258 **16 June 2004** – *Teaching the Teachers* - monthly briefing paper produced by IAAC, BP52 (IAAC, 2004f). This paper is particularly prescient given the ongoing skills crisis and attempts to address it in more recent times (2014/2015).

12.5.259 **16 July 2004** – *Transnational Co-operation in the fight against cyber-crime* - monthly briefing paper produced by IAAC, BP53 (IAAC, 2004g).

12.5.260 **16 August 2004** – *Revising Business Continuity* - monthly briefing paper produced by IAAC, BP54, (IAAC, 2004h).

12.5.261 **18 September 2004** – *Delivering IA: What needs to be done?* - monthly briefing paper produced by IAAC, BP55 (IAAC, 2004i).

12.5.262 **October 2004** - *NCC Guidelines Number 289 – Guidelines for IT management – Protect and Survive, Defending against Application Hacking, David Tracey* - defined "Application Vulnerability Testing" as a key part of a robust InfoSec management programme (NCC, 2004a).

12.5.263 **October 2004 -** *Working with Business, Your business made easy – Survey of English local authority websites from a business perspective* (UK ODPM, 2004c) - This survey concluded by stating that "most local authority websites have much to do when it comes to

providing information and services for businesses. Coverage is extremely patchy."

12.5.264 **18 October 2004** – *The changing cyber-crime threat* - monthly briefing paper produced by IAAC, BP56, (IAAC, 2004j).

12.5.265 **October 2004** – *Project Endurance – The Security Company and NHTCU launched with support from Cabinet Office and Home Office* – The Endurance mission was to bring about a change in the attitudes and behaviour of the UK's Home Internet users. It aimed to inform citizens and micro enterprises about the need for and the "how to" of basic internet security (use of firewall, anti-virus, patches, back-up) and IP (log in, phishing, etc). The initiative was developed following a Private Discussion Meeting hosted by IAAC in May 2004 and brought together interested parties from industry and government. The intentions were to provide users with information in the following areas:

- *Learn the basics: updating anti-virus and operating systems, installing a firewall;*
- *Protecting personal and financial information;*
- *Password usage and protection;*
- *Counter-fraud measures;*
- *Spyware and adware protection; and*
- *Backing-up systems.*

12.5.266 **5 November 2004 -** *Improving IT procurement: The Impact of the Office of Government Commerce's initiatives on departments and suppliers in the delivery of major IT-enabled projects – Report by the Comptroller and Auditor General, HC 877, Session 2003-2004: 5 November 2004* - Much has been put in place by the OGC to improve skills but take-up remains low. This report mentioned security at appropriate points, including the need for a Security Policy to be in place per organisation. This work is supported by various other outputs at the time from the same department (UK Office of the Deputy Prime Minister, 2002, 2003, 2004a/b/d/e).

12.5.267 **20 November 2004** – *The FoIA as a path to good IA* - monthly briefing paper produced by IAAC, BP57, (IAAC, 2004k).

12.5.268 **November 2004** - *Socitm Insight - Knock, knock: who's there? An overview of authentication for electronic service delivery, Executive briefing (Socitm Insight, 2004b)* This Briefing considers identity and authentication issues. The issue was being revisited in 2011 but this chronology shows that the issues have been fleshed out and elucidated already.

2005 - Highlights

- **March 2005 – Computer Misuse Act 1990 (Amendment) Bill issued**.
- Launch of ***Transformational Government Strategy***.
- Google Maps and Google Earth open up mapping to the public.
- **1 April 2005** – **NHS Information Authority** closed.
- BS7799 became an international standard, **ISO17799**.

12.5.269 **1 January 2005** – *Emergent European frameworks for Network and InfoSec* - monthly briefing paper produced by IAAC, BP58 (IAAC, 2005a).

12.5.270 **19 January 2005** – *EURIM – IPPR E-Crime Study, Partnership Policing for the Information Society, Building Cyber communities: Beating Cybercrime* - This report includes the following interesting statement "Governments have yet to provide their law enforcement agencies with the skills and resources to handle e-crime within their own boundaries let alone to organise co-operation across boundaries on a routine basis. Unless and until they do so, they need to provide industry and individuals with effective frameworks that enable them to work in partnership with law enforcement to protect themselves and to obtain redress". A sufficient framework existed within ISO 27001 at the time, and subsequently the National IA Strategy was launched in 2008 with a Delivery Plan that provided equally sufficient foundation to build upon. However, more time has passed since this was written and progress appears to have been slow, given the volume of mistrust in government's capability to protect and secure personal data, rather than its apparent ability to lose data and breach trust.

12.5.271 **Jan 2005 –** *SANS Beyond the Preoccupation with Certification and Accreditation* **–** *Guide to Conducting IA Systems Engineering During the Development of Tactical Systems* (Esser, 2005). The premise of this paper was that "Striking a balance between providing optimum performance and a robust IA posture is not an easy task, but can be made easier by following a disciplined IA systems engineering process and conducting critical security design activities at key points during system development" – thus alluding to the "build security in" mantra that came after this date. "This guide attempts to chart a course for the tactical system developer that interlaces crucial IA activities alongside standard DoD acquisition and systems engineering design activities, ensuring security features are standard elements of system design and life-cycle supportability plans".

12.5.272 **1 February 2005** – *Identity Management and IA, Executive Summary* - monthly briefing paper produced by IAAC, BP59 (IAAC, 2005b). IAAC had embarked on a work programme focussing on issues of Identity Management and the interrelationship with IA. This paper explains those links.

12.5.273 **1 March 2005** – *IA and the SME* - monthly briefing paper produced by IAAC (2005c), BP60.

12.5.274 **March 2005** – *Hampton Review, 'Reducing administrative burdens: effective inspection and enforcement,* (Hampton, *2005)* This report was undertaken by Philip Hampton to consider the scope for reducing administrative burdens by promoting more efficient approaches to regulatory inspection and enforcement, without compromising regulatory standards or outcomes.

12.5.275 **1 April 2005** – *Realising the Cyber-Trust and Crime Prevention* - monthly briefing paper produced by IAAC, BP61, (IAAC, 2005d).

12.5.276 **1 May 2005** – *Cyber Hood Watch* - monthly briefing paper produced by IAAC, BP62, (IAAC, 2005e).

12.5.277 **July 2005** – *Code of Practice on the Managing of Police Information (MOPI) – National Centre for Police Excellence, Home Office* (ACPO, 2005) – This has been a core piece of collateral for the police force in response to the requirements to provide advice and guidance with regard to the appropriate (and secure) management of information in all its forms.

12.5.278 **18 August 2005 –** *Professionalisation of the InfoSec industry, Nick Coleman* (Coleman, 2005a) This IAAC Briefing Paper agreed a Common Body of Knowledge (CBK) and ultimately formed the IISP. The IISP went on to develop a Skills Framework in line with the SFIA.

12.5.279 **18 August 2005** – *IA: A review of UK Government and industry initiatives, written by Nick Coleman, Chair of the Security Alliance for Internet and New Technologies (SAINT)* (Coleman, 2005b) – published by the Cabinet Office – the report "documents the development of IA in the UK and its importance to government and to industry". The definition of IA – "ensuring that data vital to the functioning of our nation is protected securely" is somewhat narrow, given the wealth available resources to provide a more robust view. However, this work identified a significant amount of effort being applied to addressing issues of achieving good IA. It was clear that "one challenge to fostering cooperation is that the groups have little knowledge of the work and activities of other groups". The subsequent mapping work identified at least 96 organisations providing advice and guidance, whitepapers, events etc in this area – suffice to say there is no shortage of resources available on the subject – potentially too many for anyone to pick a clear message from.

This was the first iteration of work done prior to the HMRC 2007 breach and is therefore supported by follow up reporting (Coleman, 2007 and 2008, King, 2008).

12.5.280 **September 2005 –** *The Public Private Boundary on the Internet,* (Internet Crime Forum, 2005) – the Legal Subgroup paper identifying key issues with regard to the changing nature of our private lives in the context of world wide web.

12.5.281 **18 October 2005** - *Identity Assurance (IdA): Towards a Policy Framework for Electronic Identity IAAC Position Paper v1.0.* This Paper pulled together the various outputs of workshops held by IAAC during the preceding year on the subject of Identity Assurance and its links with IA.

12.5.282 **25 November 2005** – *IA Governance Framework, CSIA, Cabinet Office – Working in partnership for a secure and resilient UK information infrastructure*. This was the end result of the earlier consultation and embedding the term *IA Governance – "ensuring stakeholder confidence that IS risk is managed pragmatically, appropriately and in a cost-effective manner".* This framework thus acknowledged that IA governance is "an integral element of corporate governance". IAAC had been calling for this join since early in 2002. This document addressed all the right areas. There was a section entitled *IA in the Procurement Process* that reflected "A project fails if it does not meet its IA objectives, since the information delivered by the service and upon which the business relies may not be adequately protected..... This can only be achieved by treating the IA requirements applying to the system or service as an integral element of the business throughout the entire procurement process". However, the document confuses "a specific security policy statement" with "a Risk Management and Accreditation Documentation Set [RMADS]" – these are not the same thing – and in many ways there is a translation service required in order to understand the totality of the framework – if you are not "au fait" with government security standards and publications you might struggle to know how best to progress with the content provided therein (Original consultation in 2004 – UK Cabinet Office, 2004a).

2006 - *Highlights*

- 25 January 2006 ***– Police and Justice Bill –*** included set up of the National Policing Improvement Agency (NPIA).
- IAAC launch of ***ID Assurance programme***.
- Guardian ***Free our Data*** campaign begins.
- ***EU Inspire Directive for Open Spatial Data***.
- Confidence as a concept is added into the IA rhetoric.
- PCI Security Standards Council is born – as a Standards setting body NOT as an *enforcement* body; enforcement is driven out through the "brands".
- Wikileaks founded by Julian Assange - https://wikileaks.org/

12.5.283 **30 January 2006 -** *Transformational Government in a responsible way - IAAC Response to the Cabinet Office consultation paper on Transformational Government – Enabled by Technology.* This report contained the following: 'The Government will further develop its risk management model'. In developing this model it is important to take explicitly into account the risks resulting from joining up previously stove piped systems. However, the transfer of risk between departments is not well handled, as shown by the Bichard Report.

This was considered to be a general governance level issue that should be addressed, explicitly. In the Strategy, government expressed its ambition of developing a holistic approach to identity management, which should enable provision of trusted services (par.39/7). It also announced a new Ministerial focus on finding and communicating a balance between privacy and efficiency with respect to data sharing (par. 39/4).

In order to support developing insight in this, IAAC rolled out a consultation process in which government and industry stakeholders met with academia and international experts.

The intention was to deliver an Identity Assurance Roadmap for the UK by July 2006, which would aim to provide a baseline insight and inform government and industry policy making.

12.5.284 **2006** – *Information Governance in the Department of Health and the NHS – Cayton,* "The coherence, clarity and consistency in the way information is governed within and between the various bodies involved in the development, delivery and monitoring of NHS care and services will need to be improved to support an electronic NHS."

12.5.285 **May 2006 –** *Pervasive Computing* – a *Parliamentary Office of Science and Technology* "postnote" publication, Number 263 (UK Office of Parliamentary Science and Technology, 2006a) addressing this topic. Privacy, safety, security and technology issues were all identified at the time.

12.5.286 **June 2006** - *IA in a Global Bank, Stephanie Daman presentation to BCS Bimingham IT Security Conference, HSBC Holdings plc (Daman, 2006)* - Daman (a long standing and active IAAC member) provided what has to be *the* most comprehensive and clear definition of IA. "IA is the confidence that the information assets with an organisation are reliable, accurate, secure and available when required. IA:

- *Includes information held in every form (IS, on paper, other records, speech);*
- *Embraces IM, including InfoSec management, information and records management, data protection, privacy (because of close confidentiality links and Organization for Economic Co-operation and Development [OECD] guidance requirements) and physical protection;*
- *Must be maintained throughout an organisation's lifecycle in the face of changing threats, vulnerabilities and dependencies;*
- *Includes aspects of corporate governance, risk management and business continuity (resilience); and*
- *Ensures that information is fit for purpose".*

12.5.287 **July 2006** - *Roadmap for Identity Assurance in the United Kingdom* (IAAC, 2006). This was the anticipated Roadmap which described identity as "*a collection of attributes which helps to distinguish one entity from another*". This is what makes identity a key component in numerous economic, social and political transactions.

12.5.288 **July 2006** – *Hi-Tech Investigative Research: The illicit trade in Pharmaceuticals* (Wright, 2008b) – detailed analysis for the City of London Police by Detective Sergeant Paul Wright.

12.5.289 **10 August 2006** – *A United Kingdom Strategy for IA – Cabinet Office* The first sentence stated that "Information is a critical asset for any organisation". The vision for this strategy was "to enable a UK environment where citizens, businesses and government have confidence that IS enable them to conduct their lives and businesses more efficiently, flexibly and safely.

Individuals and organisations have realised the full benefits of ICT through IA which is embedded within the culture of organisations and is an invisible but indivisible part of the everyday processes driving business delivery."

12.5.290 **September 2006** - *Call for Evidence by the House of Lords on Personal Internet Security.* This was the beginning of a volume of relevant work, identifying the concern of the average citizen that all may not be well in the internet space in terms of the protection of their privacy and the security of their personal data.

12.5.291 **September 2006** – *UK Information Commissioner's Office (ICO, 2006) A Report on the Surveillance Society for the Information Commissioner by the Surveillance Studies Network, Full Report*. The now infamous line "sleepwalking into a surveillance society" was borne around this time as a result of the increased media attention in the subject area.

12.5.292 **September 2006 –** *IAAC Symposium* Lord Toby Harris suggested a Consumer Bill of Rights with the core premise that *Every citizen and consumer has a right to demand protection of their data:*

a) *"Don't Give Others My Data Without My Permission" – This raises interesting questions for the management of identity and the issue of user control and usage transparency for government.*

b) *"Don't Lose My Data" – It is extremely inconvenient (an understatement) when this happens in electronic environments, as it can have very detrimental effects, even devastating, on the person whose information goes missing.*

c) *"Don't Abuse My Data" – This is fundamental for the establishment of robust frameworks to regulate the use of data, preventing inappropriate or illegitimate use.*

d) *"Don't Waste My Time" – How to handle processes such as authentication in the most efficient manner, to avoid repetition and duplication? Reducing the inconvenience to users should be a key concern.*

e) *"Can I Prove Who I Am and Can You Prove Who You Are?" – This is about getting the processes of establishing identity right, in particular at the stages of registration and authentication.*

f) *"Can You Be Assured That The Information Provided Is Accurate and If Not, Can It Be Corrected?" – Again, a challenge particularly for the provision of public services.*

However, within the above a number of issues must not be forgotten. The right to demand protection of your personal data is enshrined within the Data Protection Act (DPA) 1998 – that is rather the point of

it. The ability to address any corrections requirements is also account for in the DPA 1998. The DPA also already provides individuals with the right to control who has access to their personal data. However, the deployment of technology and processes is not necessarily in keeping with the most appropriate legislative compliance in this regard. Hence, the most recent changes with regard to cookie collection under the EU Electronic Communications Framework.

12.5.293 **October 2006 –** *Data Encryption* – a *Parliamentary Office of Science and Technology* "postnote" publication (Number 270) addressing this topic. Legislation, reliability concerns and drawbacks were all discussed (UK POST, 2006b).

12.5.294 **October 2006 –** *Computer Crime* – a *Parliamentary Office of Science and Technology* "postnote" publication (Number 271) addressing this topic. Legislation, user awareness and policing issues were all identified (UK POST, 2006c).

12.5.295 **November 2006** – *Regulatory Justice: Making Sanctions Effective, Professor Richard B Macrory.* Every area of the public sector was subject to some level of scrutiny of their information-based practices, in particular seeking to improve efficiencies and enhance effectiveness.

12.5.296 **November 2006** – *Managing your risk appetite: A practitioner's guide*, published by HM Treasury. This publication robustly discusses risk appetite as a required output of risk assessment and emphasises the need to ensure that the board's attitude to risk must be appropriately cascaded throughout any organisation.

12.5.297 **December 2006** – *Varney Report, Service Transformation* (Varney, 2006) – The "language" was beginning to change. This report contained significant reference to identity management systems but no direct mention of InfoSec nor IA. However, it did mention "security considerations", "safety and security practices", "security issues" and "security and privacy", though all *still* "ICT security" focussed. "Government needs to move quickly to a rationale on proportionate sharing of identity information which respects privacy". The stated intention "beyond 2012" is that "the public and private sectors are converging on a common identity management regime that puts the UK at the leading edge of international practice and commands high levels of public confidence about good service, security and privacy". This is critical to bear in mind given the cancellation of the Identity Card Scheme after the May 2010 election and the subsequent search for a suitable "home" (government sponsor or otherwise) for progressing with a sensible identity management platform for the country as a whole.

2007 – Highlights / Lowlights

- **May 2007** – IAAC took part in the ***IA Strategy*** review.
- ***July* 2007** – ***Cabinet Office Power of Information Review*** (reporting not until 2009).
- During **2007/2008** – there were serial breaches of both information security and data protection.
- **Identity Assurance** focus.
- Cabinet Office **Power of Information** Review.
- The Regulation of Investigatory Powers (Investigation of Protected Electronic Information: Code of Practice) Order 2007.
- NIAS updated.
- Several high profile data breaches, including the HMRC Child Benefit Data Loss.

12.5.298 **10 January 2007** – *HMG Transformation Government Enabled by Technology, Annual Report 2006 (UK Cabinet Office, 2005c).* This report contained lots of reference to information and data sharing but no real references to InfoSec nor IA.

12.5.299 **30 January 2007** – *IA Risk and Decision Makers* The BCS Security Forum hosted a "Hot Topics" debate at which Lt Gen Sir Edmund Burton, Professor Brian Collins (Department for Transport), Dr Paul Dorey (BP, at the time) and John Smith (Prudential) all spoke about the need to communicate the importance of risk management to decision makers, to engage with them and to move the dialogue forward.

12.5.300 **February 2007 –** *Internet Governance* – a *Parliamentary Office of Science and Technology* "postnote" publication, Number 279 (UK POST, 2007a) addressing this topic. The Internet Governance Forum was highlighted in the paper – the group first met in October 2006.

12.5.301 **February 2007** – *ETSI White Paper No. 5: ICT Product Proofing Against Crime* – addressed the Five I's: Intelligence; Intervention; Implementation; Involvement and Impact, across the CRAVEN characteristics of "hot products":

- *Concealable;*
- *Removable;*
- *Available;*
- *Valuable;*
- *Enjoyable and*
- *Disposable.*

12.5.302 **5 March 2007** – *Statistical Data on Network Security* – a report produced by the European Commission detailing the prevailing trends. This makes for interesting reading a decade later.

12.5.303 **March 2007** – *Business Leadership of Technological Change – Five key challenges facing CEOs* - This Cranfield University sponsored study highlighted the need for business leaders to create networks

for knowledge sharing amongst each other and beyond and to ensure that they undertake personal learning, given that the commitment to staying on top of the information age requires making the time available to do so. This is important learning for the professionalism agenda (Tranfield and Braganza, 2007).

12.5.304 **21 May 2007** – *Delivering the IA Strategy,* New Structure Version 1.10. The Strategy puts IRM at Board level (UK Cabinet Office, 2007c).

12.5.305 **June 2007** - *IA07: A Partnership for Delivering the National IA Strategy - A delivery plan document used for discussion at IA07.* This document stated that the framework "is to be fully implemented by 2011" so there is some catching up to be done. "The private sector is encouraged to overcome the challenges to sharing IA best practice for their own benefit and that of their customers and to expand the reuse of technology;" – this completely misses the point that the barriers are often not within the gift of the private sector to resolve as they are bound up in the legal requirements and statutory obligations of the public sector body they are seeking to partner with. "Business and industry will provide training and information so that all staff have a basic understanding of IA and its implications". The reality is, of course, that the private sector is happy to provide the services but nobody is buying much at the moment, nor spending the money on this as the economic downturn continues and so often it can be seen that training budgets are slashed so the ongoing training provision is floundering.

IRM: Ownership of IA at Board level - Successful management of information risks is helped by an organisational culture where people appreciate IA. The IA Board representative will ensure that training is provided and that everyday IA processes and procedures are organised effectively.

Standards and Compliance

- *Adhering to a framework of segmented national IA standards developed by government IA specialists working together with key industry stakeholders. This will likely include best practice industry standards (e.g. ISO 27001) and regulatory instruments in commercial contracts;*
- *Use of specific tools, such as criteria for deciding whether information is critical or not coupled with records of tested and approved security solutions;*
- *Internal audit to monitor compliance, develop performance metrics and compliance tracking.*

Other key elements were fleshed out as represented in the action plan in Figure 93 below.

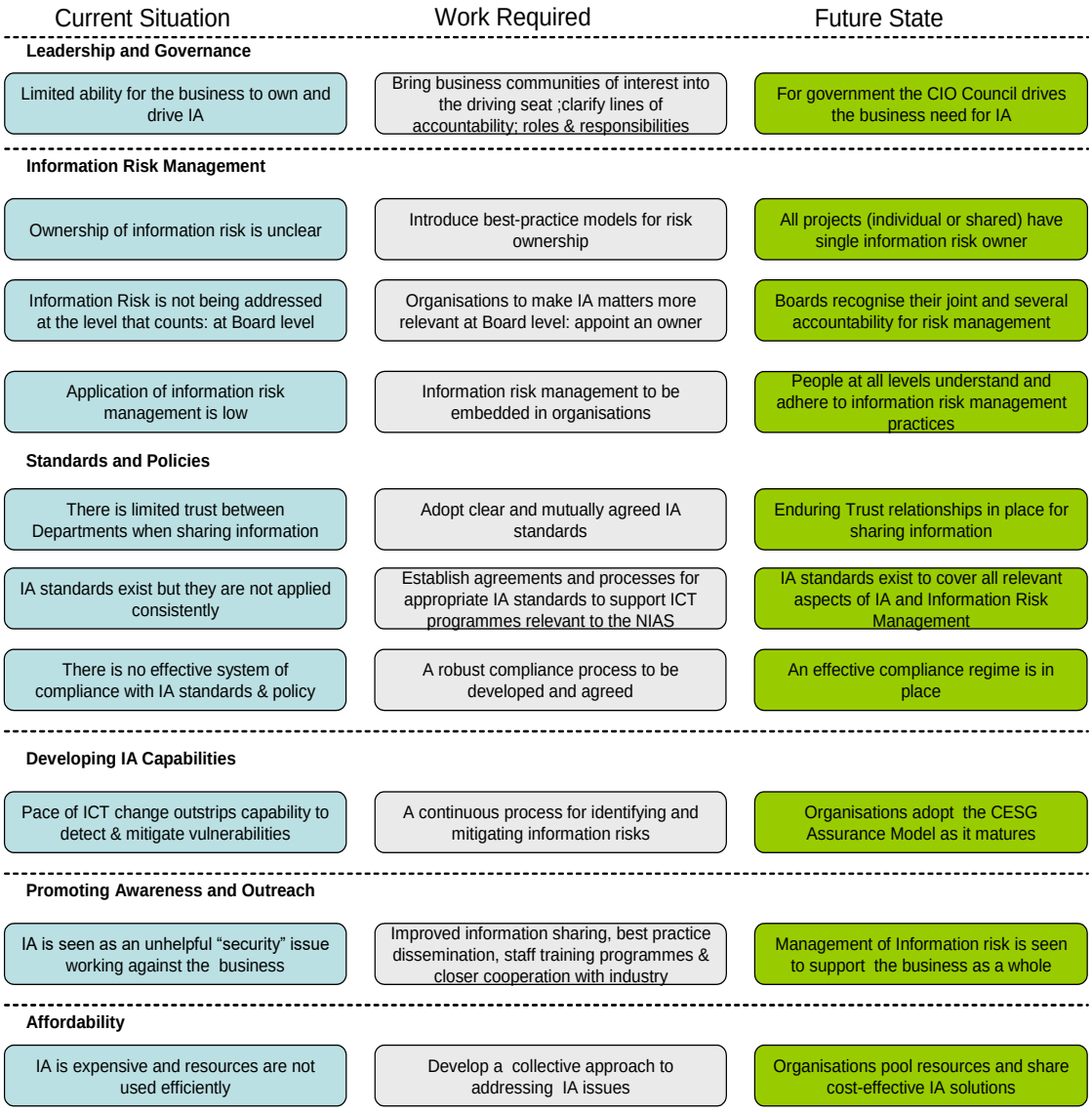


Figure 93: Delivering the IA Strategy, Source: UK Cabinet Office (2007c)

12.5.306 **22 June 2007** - *National IA Strategy* re-launched. It reinforced the mantra that "information is a valuable asset". The Strategy provided alignment with the Transformational Agenda. It defined IA as being "the term given to the management of risk to information" – which is a somewhat interesting (and unnecessary) tweaking to the already existing definition(s) of IA. "This NIAS sets out a coherent approach to management information risk (sic) by making it an integral and effective part of normal business process". It acknowledged the role played by the private sector in achieving government policy and the challenges this creates. The aim was to create a "UK environment where citizens, businesses and government use and enjoy the full benefits of IS with confidence. Note this was shortly before the HMRC data breach that brought such confidence (and the potential diminishment of such) into sharp focus in the mind's eye of the entire UK public.

12.5.307 **June 2007 -** *Confederation Suisse IA Situation in Switzerland and internationally, Semi-annual report* 2007/1 (January – June), Feder Office of Police. This is a classic example of a report with IA in its title that has content that is specifically InfoSec related and is wholly about *just* the technical aspects (virus increase, Trojans, worms, hacking incidents etc.). It is misleading and misrepresentative of the subject area but is included in this review as an example of the kind of information available and being shared in the e-crime space that has an impact on the development of public policy to support the requirements that needed to be addressed.

12.5.308 **July 2007** – *IATAC State of the Art Report* (IATAC, 2007) – discusses Software Security Assurance historically and to the present day and yet 8 years later the challenges and opportunities remain largely unresolved with evidence of greater risks, threats and resultant breaches being realised.

12.5.309 **July 2007 –** *Grids and e-Science* – a *Parliamentary Office of Science and Technology* "postnote" publication, Number 286 (UK POST, 2007b) addressing this topic. Grids were identified as being useful for dealing with increasing amounts of data produced by science, business and government. This was prior to the marketing term, "Big Data".

12.5.310 **14 August 2007** – *Government's Role in Identity Assurance* - monthly briefing paper produced by IAAC, BP63 (IAAC, 2007a).

12.5.311 **September 2007** – *Cyber-Crime Investigation and Enforcement; Designing Out E-Crime: Removing vulnerability and reducing temptations* and *From Awareness to Action? On-Crime Prevent Programmes* (EURIM 2007) – a EURIM co-ordinated set of papers providing detailed analysis of the available resources and partnership working.

12.5.312 **November 2007** – *Data Loss Prevention: A Time to Revisit Old Policies* – a Symantec paper addressing policy and procedure review following data breaches.

12.5.313 **7 December 2007** – *National IA Strategy* - monthly briefing paper produced by IAAC, BP64 (IAAC, 2007b).

12.5.314 **December 2007** - *Privacy Impact Assessment handbook and surveillance society conference* (ICO, 2009) - The Information Commissioner's Office hosted a conference entitled 'Surveillance Society: Turning Debate into Action' at the Bridgewater Hall in central Manchester.

12.5.315 **December 2007 –** *China: Reducing Your Vulnerability to Commercial Espionage* (Security Information Service for Business Overseas, 2007) – a reporting detailing the threat to Intellectual property and technology in China – on the premise that "awareness is half the battle".

12.5.316 **December 2007** – *Cyber Attack: A Risk Management Primer for CEOs and Directors* (Atlantic Council, 2007) – business focussed and talked about the need to create a security culture.

12.5.317 **December 2007** – *Data Handling Procedures in Government: Interim Progress Report,* issued by Robert Hannigan (UK Cabinet Office, 2007d).

2008 - Highlights

- Amended ***Computer Misuse Act*** (CMA) came into force
- GRC a more oft used acronym.
- First UK National Security Strategy.
- Revision of Data Handling Procedures.

12.5.318 **1 February 2008** – *The Needs and Concerns of the Citizen* - monthly briefing paper produced by IAAC, BP65, (IAAC, 2008a).

12.5.319 **1 February 2008** – *How UK Government can Gain Citizen Support* - monthly briefing paper produced by IAAC, BP66 (IAAC, 2008b).

12.5.320 **20 March 2008** - *The National Security Strategy of the United Kingdom, Security in an interdependent world* - This is an interesting and important document but contains no direct reference to IA. It highlighted that:

- *"Britain today is both more secure and more vulnerable than in most of her long history.*
- *More secure, in the sense that we do not, currently, have to face a conventional threat of attack on our territory by a hostile power.*
- *But more vulnerable, because we are one of the most open societies, in a world that is more networked than ever before, with new threats that can emanate from state and non-state actors: terrorists, home-grown or overseas; insurgents or criminals.*
- *Terrorism, cyber-attack, unconventional attacks, using chemical, nuclear or biological weapons, as well as large scale accidents or natural hazards – any one of these could do great damage to the country" (Burton, 2011).*

12.5.321 **2 April 2008** – *Guidelines for the cooperation between law enforcement and internet service providers against cybercrime* – produced by the Council of Europe.

12.5.322 **25 April 2008** – *Canadian Association of Police Boards – A Report on cybercrime in Canada* – produced by Deloitte, reviewed the changing trends of criminal activities, the lack of reporting and the perceived lack of support from law enforcement.

12.5.323 **1 May 2008** – *Citizen Control* - monthly briefing paper produced by IAAC, BP68 (IAAC, 2008c).

12.5.324 **1 May 2008** – *Digital Identity Governance Framework* - monthly briefing paper produced by IAAC, BP69 (IAAC, 2008d).

12.5.325 **5 May 2008** - *UK State of Security (A high level overview of the players and roles that govern security within the UK)*, by Gareth Niblett. This paper set out a full A-Z of all those who have an "interest" in areas of "security" within the UK in the form of a catalogue listing the following:

- *Government Interests*
- *Law Enforcement Interests*
- *Military and Intelligence Interests*
- *Organisational Interests*
- *Industry Interests*
- *International Interests*
- *Academic Qualifications*
- *Product Certifications*
- *Professional Certifications*
- *Technical Accreditations*
- *United Kingdom Legislation*
- *European Directives*
- *International Agreements*
- *United States Legislation*
- *Regulations*
- *United Kingdom Standards*
- *International Standards*
- *Methodologies.*

In many ways, given efforts that went on in late 2010 to gather together similar levels of data, this was a valuable resource that should have been kept up to date. There is a great capacity to do things on a snapshot basis rather than investing sufficient energy in the appropriate maintenance of the wealth of available material.

12.5.326 **23 May 2008** – *Hi-Tech Crime Strategy and Budget for 2011* - robust paper identified both the scope of the problem space and suggested recommendations for tackling the identified issues for the *UK City of London Police* (Wright, 2008a).

12.5.327 **May 2008** – *Insecure Internet Access via wireless*, Detective Sergeant, Hi-Tech Crime Team, City of London Police (Wright, 2008c) - Recommending the creation of e-crime prevention officers.

12.5.328 **10 June 2008** – *Insecure Internet Access via Wireless* – this report highlighted the need for partnership between the public and private sector in the future in order to help to address the increasing threat of cybercrime.

12.5.329 **June 2008** - *Data Handling Review* - This report put in place a set of mandatory measures for government on protecting personal data, committing government to report annually on the progress made in meeting the requirements of the review and work on information risk that will be necessary in the future. (There was an interim report in

December 2007). (UK Cabinet Office 2007c, 2008a, 2008d, UK CSIA, 2008).

12.5.330 **June 2008** – *Data Handling Procedures in Government* (UK Cabinet Office, 2007d, 2008a) - This was the final report on data handling procedures across government. The report set out how government was improving its arrangements around information handling, management and protection.

12.5.331 **11 June 2008** – *Improving internet safety* – a paper written by the Security Forum of JANET UK to address the trends and concerns at the time. The key theme was the ability to establish ownership for the identified responsibilities.

12.5.332 **June 2008** - *Protecting Government Information, Independent Review of Government IA* (Coleman, 2008). This report was the result of Nick Coleman's independent review during 2007 where the key question asked was "How well is government doing?" – i.e. is IA adequate enough across government to provide stakeholder confidence in the government's IA? The issuance of the final report itself ended up being delayed as a result of the October/November 2007 HMRC data breach. There were 10 key recommendations put forward, much of which were picked up in the Data Handling Review itself and these were also embedded in the Code of Connection requirements on many public sector organisations in joining up to the central government networks. The following Computer Weekly opinion piece (King, 2008) rather sums up the state of affairs:

> *The list of recommendations makes for equally gloomy reading. Here is why. We've been talking for years, even decades, about the need for strong InfoSec governance, accountability, and setting minimum standards. This is nothing new. But here we are heading towards the end of the first decade of the 21st century and a report about and for the Government - the highest authority in the land - is highlighting a need to "***Define minimum standards that (public sector) departments sign up to***". Good grief. What on earth have they been up to all these years? If there were a book entitled "InfoSec for dummies" then that would be on page 1. It shows just how far behind the public sector is and makes for good explanation as to why it is subjected to so many data breach incidents."*

12.5.333 **July 2008** - *Report into the Loss of MoD Personal Data* - Sir Edmund Burton's review (Burton, 2008). This included MOD's action plan in response to the report, supported by the MoD Action Plan (UK MoD, 2008).

12.5.334 **July 2008** - *Poynter Review* (Poynter, 2008) - The final report by Kieran Poynter, the Chairman and Senior Partner of PricewaterhouseCoopers, on the circumstances that led to the significant loss by HMRC. [**Note**: the recommendations from the various reports are readily available and Simmons (2009) wrote specifically about how best to utilise these and achieve best practice.]

12.5.335 **11 July 2008** – *Internet Governance Forum* – a paper written by Shriti Vadera, at the time, Parliamentary Under-Secretary of State for Business and Competitiveness. This was a detailed review of the use of internet at the time for sharing views with regard to significant global political elections.

12.5.336 **July 2008** - *Cross Government Actions: Mandatory Minimum Measures* (UK Cabinet Office, 2008d) - A core set of mandatory minimum measures to apply across central government to protect information. Measures for the protection of personal data were subsumed within IA Standard No 6 – HMG Security Policy Framework (SPF) mandatory requirement 14 (UK Cabinet Office, 2009e, f and g). This went through several updates and revisions, the last known being in 2013.

12.5.337 **July 2008 –** *Consultation on Legislative Options to Address Illicit Peer-to-Peer (P2P) File-Sharing* – a comprehensive report into this prevailing issue at the time (UK BERR, 2008).

12.5.338 **2008** - *Managing Information Risk, A guide for Accounting Officers, Board members and Senior Information Risk Owners* - This Guide provided Plain English Information Risk descriptions including the "human dimension" (now referred to as *human factors*) and included a number of helpful checklists. The language was clear and easy to understand (UK HMG 2008a).

12.5.339 **September 2008 -** *UK Cybercrime Report* – identified the difficulty of addressing the problem whilst not having government level responsibility for collating and classifying cybercrime data adequately addressed (Fafinski and Minassian, 2008).

12.5.340 **16 October 2008** – *Parliament and Internet Conference E-Crime Reduction Partnership workshop report (EURIM)* – addressing the national e-crime strategy vision of effective partnership working across the Police Central E-Crime Unit (PCEU), the Fraud Authority and the e-Crime Reduction Partnership. Global partnerships were identified as a further outreach requirement.

12.5.341 **November 2008 -** *Information Matters: building government's capability in managing knowledge and information* (UK HMG 2008b) was published by The National Archives in conjunction with the Knowledge Council, addressing the importance of management of knowledge and information and the need to improve in these areas. Government was advised to regard the management and exploitation of knowledge and information as a core responsibility, supporting business objectives and delivering business benefits. This strategy built on a number of similar initiatives in relation to different types and uses of information. There should not be significant additional cost associated with delivering the strategic objectives outlined here, but there should be tangible benefits.

12.5.342 **November 2008** – *Taking Stock, Taking Action* (UK ICO, 2008a) – *ICO report* As the ICO rightly phrases it, "information governance" or the apparent lack thereof is the bigger issue – at an executive level, along with a lack of leadership.

12.5.343 **26 November 2008 -** ICO's *Privacy by Design* (UK ICO, 2008b) report and conference.

2009 – Highlights / Lowlights

- Tim Berners-Lee "Raw data now" speech at TED.
- Tim Berners-Lee appointed as expert advisor by Gordon Brown.
- US federal and state open data stores – data.gov, datasf.org etc.

12.5.344 **12 January 2009** – *Top 25 Most Dangerous Programming Errors* – produced by Mitre's Common Weakness Enumeration (CWE) in conjunction with SANS. It leverages the existing SANS Top 20 attack vectors. It is a consistently well-known fact that there are obvious steps that can be taken to reduce the likelihood of the impact of or the realisation of a known threat.

12.5.345 **February 2009** - *Power of Information Taskforce Report (*UK Cabinet Office, 2009a) was published – aiming to look at the ways in which government can improve its use of digital technologies and information. The *Making Public Data Public* initiative will deliver improved access to public information both in central government and the wider public sector.

12.5.346 **February 2009** - Tim Berners-Lee (TBL) "Raw data now" speech at TED. Subsequently, TBL was appointed as an expert advisor by Gordon Brown. The reflection at the time was on dealing with US federal and state open data stores (data.gov and datasf.org etc) and advising that the UK Government should adopt the same approach to opening up their raw data stores for wider usage and exploitation. TED stands for Technology, Entertainment and Design. It started out (in 1984) as a conference bringing together people from those three worlds. Since then its scope has become ever broader (Berners-Lee, 2009).

12.5.347 **March 2009** - *Building in...InfoSec, Privacy and Assurance – a high-level roadmap* (Jones, 2009), Nigel A Jones, Director Cyber Security KTN – IAAC participated in the formulation of this. The roadmap sought to deliver on the following vision: "The development and procurement of software and systems which are resilient and sustainable by design, where requirements such as security and privacy are, as a matter of course, defined at project initiation and implemented and assured throughout in risk-based, whole-life processes". In fairness, the Information Commissioner had set about a similar course in November 2007 but was overshadowed by the HMRC data breach.

12.5.348 **March 2009 –** *Database State Full Report* (Joseph Rowntree Reform Trust Ltd, 2009), commissioned by the Joseph Rowntree Reform Trust Ltd, issued 23 March 2009. A meeting of academics and activities with an interest in privacy attempted to map Britain's database state, identifying the many public sector databases that collect personal information, and provide a traffic light colour grading to their abilities to adhere to the UK Data Protection Act Principles.

12.5.349 **May 2009** – *IA Standard 6 (IAS 6)* This is part of UK Governments Security Policy Framework (SPF). SPF is a response to government data breaches uncovered in the government's Data Handling Review. IAS 6 requires all government agencies to submit reports of compliance to the UK Cabinet Office to prove that the methods they use to process and store sensitive personal information are secure. The original reporting deadline was 15 June 2009. IAS 6 is supported by Good Practice Guide 15, which is published by the UK Cabinet Office and the Communications-Electronics Security Group (CESG). CESG gives a more prescriptive explanation of not only the data that must be collected for the report, but also how to collect it.

12.5.350 **June 2009** - *"Digital Britain Report" published* (UK DCMS, 2009), aiming to secure the UK's position as one of the world's leading Digital Knowledge economics, recognising that the digital world is now a reality.

12.5.351 **June 2009** - *Office of Cyber Security* (OCS) launched. As well as cyber-defence and cyber-attack coordination, the OCS will act as a conduit for InfoSec collaboration between government and industry experts. The OCS will have charge of a cross-government programme of work, while a multi-agency Cyber Security Operations Centre (CSOC), based at GCHQ in Cheltenham, will coordinate the protection of critical IT systems.

12.5.352 **June 2009** - *National Cyber Security Strategy* published in order to ensure that "Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience". This was a consultation in advance of the actual Strategy which was launched in March 2010 (UK Cabinet Office, 2009b).

12.5.353 **July 2009** - *Power in People's Hands: Learning from the world's best public services* This report addressed the need for UK public services to innovate rapidly and to learn from the best services around the world (UK Cabinet Office, 2009c).

12.5.354 **July 2009** – *IA09 Conference Special* – UK Government's IA event review. Topics for discussion included the recently released UK Government Cyber Security Strategy and the CESG approach to defining what constitutes an IA practitioner.

12.5.355 **October 2009 -** *Government ICT Strategy,* (UK Cabinet Office, 2009e). The strategy explicitly covered InfoSec and IA stating that "Recent data losses within the public sector have rightly raised the profile of IA. However, without appropriate levels of data sharing, Government will be unable to meet its aim of joining up services and providing easier access to personalised services for citizens and businesses. Effective, proportionate management of information risk is essential to meet the challenge of delivering personal services enabled by ICT, as well as making us more effective and efficient. Work to enhance InfoSec and IA through the National IA Strategy cuts across all elements of this ICT strategy and is embedded within all work-streams. The ICT strategy will deliver a secure and proportionate infrastructure that will allow public sector bodies to match their information risk appetite with their information risk exposure - users of that infrastructure will be able to take IA for granted without feeling that their effectiveness has been compromised". Published in January 2010.

12.5.356 **December 2009** - *Putting the "Frontline First: Smarter Government"* addressed the rebalancing of the relationship between "the centre and the frontline" (UK HM Treasury, 2009a).

2010 – Highlights / Lowlights

- **Jan** - data.gov.uk and data.london.gov.uk launched.
- **Apr** - Ordnance Survey makes some mapping data open.
- **May** - David Cameron letter re central and local data transparency.
- **May** - Tim Berners Lee, Nigel Shadbolt and Tom Steinberg appointed to Cabinet Office Transparency Board.
- **Jun** - Eric Pickles announces local government publication of £500+ spend/contracts by Jan 2011.
- **Oct** - UK Open Government Licence released.
- **Oct** - Ordnance Survey makes more mapping data open.
- **Oct** - David Cameron and Francis Maude reiterate support for open data.
- **This decade includes mobile devices, cloud computing, the semantic web, Twitter and the Internet of Things**.

12.5.357 **January 2010** - **"***Protecting Information in Government***"**. The first "annual" report from the Cabinet Office on its implementation of the Data Handling Review Acknowledgement that managing information risks is an ongoing task (UK Cabinet Office, 2010a).

12.5.358 **January 2010** – *Government ICT strategy: smarter, cheaper, greener*. The strategy applies to the UK public sector, whether central government, local government, wider public sector or devolved administrations. It is aligned with the *Transformational Government* and *Digital Britain* strategies, the *National IA Strategy,* the *Cyber Security Strategy, Building Britain's Future, Excellence and fairness,* the *Operational Efficiency Programme* (OEP) and the

recommendations of the Power of Information Task Force (UK Cabinet Office, 2010b).

12.5.359 **January 2010 -** data.gov.uk and data.london.gov.uk launched as the early fruits of TBL labour etc.

12.5.360 **March 2010** – *Cyber Crime Strategy* launched (UK Home Office, 2010).

12.5.361 **March 2010** – *ISACA COBIT 5.0 Design Paper Exposure Draft* issued. This is the starting point for the maturation in ISACA thinking in the area of IT Governance, where the professionals involved have rightly seen that the growth in the assurance framework areas leads to a need for greater IG and their new standard seeks to capture these strands. This paper points out that "Effective enterprise governance of IT results in improved performance as well as compliance to external requirements, yet successful implementation remains elusive for many enterprises. Processes need to be supported with carefully prescribed roles, responsibilities, and accountabilities. They also require an appropriate set of guiding principles and organisational structures that fit the culture, style, skills and operational norms specific to the enterprise, inclusive of all stakeholders and role players". There is a strong strand on ethics and culture in the resultant product (ISACA, 2010b).

12.5.362 **April 2010** - *Ordnance Survey* - makes some mapping data open.

12.5.363 **April 2010** - *Busy Reader Guide for Improving IA at the Enterprise Level CESG National Technical Authority for IA* (UK CESG, 2010c). This Briefing puts forward the case for improving IA at an Enterprise level in a short and concise manner. It is easily readily and digestible and has a checklist at the end that is actionable. In particular, this Briefing places IM as being important in the IA space. It also includes the clear Enterprise level approach required – and the notion that HR need to ensure they are prepared to address non-compliance.

12.5.364 **May 2010** - David Cameron letter regarding central and local data transparency to LA CEOs – the new Coalition government set out its stall with regard to intending to ensure greater transparency of information and transactions across the public sector.

12.5.365 **12 May 2010** - Government plans to scrap £15bn of IT projects – the new Coalition government moved quickly into action mode in setting out its plans for the future of Government IT projects and spend.

12.5.366 **25 May 2010** - *A Freedom or Great Repeal Bill* was discussed. By 2011 this had changed to a *Protection of Freedoms Bill*.

12.5.367 **27 May 2010** – *HMG IA Maturity Model and Assessment Framework* (UK CESG 2010i), Version 4.0 issued by UK Cabinet Office and CESG, with three main IA goals identified below and an Assessment framework to be utilised for measuring maturity, measured on a five level maturity scale (Level 1 - Initial; Level 2 - Established; Level 3 –

Business Enabling; Level 4 – Quantitatively Managed; Level 5 - Optimised:

- *Embedding IRM Culture within an Organisation*
- *Implementing Best Practice IA Measures*
- *Ensuring an Effective Compliance Regime is implemented.*

12.5.368 **June 2010** - Eric Pickles announces local government publication of £500+ spend/contracts by January 2011.

12.5.369 **July 2010 -** *Requirements for Secure Delivery of Online Public Services Part 1 Principles and Part 2: Security Components* (UK CESG, 2010d/e/f and 2012a). This weighty tome revised, repositioned, and set out to replace the E-Government Security Framework (e-GSF) last updated in 2002. Part 1 (Principles) describes the scope, context and the approach to be followed in determining security requirements for future public service systems. Part 2 (Security Components), this part, describes the security components that are used to express the security requirements. At 122 pages long, this is a significant document, particularly given it is ultimately ISO 27001 and other best practice combined and reworded.

12.5.370 However, both documents were issued quietly in the summer and have had no real "air time" or follow through as yet (March 2011). The following key chapters are of note:

- *Chapter 2 End user security components – this chapter covers the security components relevant to the people and businesses accessing the service;*
- *Chapter 3 Server security components – this chapter covers the security components relevant to the ICT hosting the service;*
- *Chapter 4 Network security components – this chapter covers the components relevant to the network infrastructure which is used to access the services;*
- *Chapter 5 Business logic security components – this chapter covers the components relevant to the software application that implements the service;*
- *Chapter 6 Assurance security components – this chapter covers the components relevant to gaining confidence in the end-to-end security of the public sector services (UK CESG 2010d and 2010e).*

12.5.371 **October 2010 -** *UK Open Government Licence* released – which will support the framework for publication of information in the context of the "Raw Data Now" requirements.

12.5.372 **October 2010** – CPNI issued ***Sources of Guidance on Security in the Telecommunications Sector*** – a helpful compendium single source for the publicly available advice, guidance, standards, good practice, best practice etc, relating to the security of telecommunications systems.

12.5.373 **October 2010 -** *Ordnance Survey* makes more mapping data open – this has been a necessary step following the amount of available data through the ongoing progress of Google Maps.

12.5.374 **October 2010 -** *David Cameron and Francis Maude reiterate support for open data*, making recommendations to Local Authorities as to how to go about achieving this.

12.5.375 **Late 2010** - *Office of Cyber Security and IA* formed. After a decade of discussing and seeking to implement IA, following the election of the UK Coalition Government, the CSIA became known as the Office of Cyber Security and IA (OCSIA 2011). This appears to the author to be a subtle hint towards the difficulties in having to constantly explain what IA is and what it means – without the context of InfoSec - as well as a perceived need to keep in step with the media thinking in terms of "hot topics" that "sell" the story on any particular day.

12.5.376 **December 2010** - *A Taxonomy of Operational Cyber Security Risks* (Cebula and Young, 2010). Given that this is a CERT publication from the Carnegie Mellon Institute, renowned as being a source of core knowledge in most subject areas related to the security industry, it is particularly disappointing in review of the report to find that whilst purporting to present a taxonomy of *operational cyber security risks* – there is nothing *specifically* cyber in nature about the risks presented. However, the report does helpfully identify and organize the sources of risk into four *classes*: (1) actions of people, (2) systems and technology failures, (3) failed internal processes, and (4) external events and is a good general resource for "security risks" per se, but not explicitly "cyber" risks and is another example of how the hijacking of the term does a disservice to the reality of what is being described. Within the document, "*Operational cyber security risks"* are defined as "operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or IS" – so, these are rather *InfoSec* risks then, and there is no need for the flagrant use of the "*cyber*" term.

2011 Highlights / Lowlights

- A year of civil and cultural uprising; "Arab Spring", Occupy Wall Street and beyond etc....; 2014 = year of breach/data loss.
- Cybercrime cost the UK economy £27bn a year, UK OCSIA and Detica Report, February 2011 – The Cost of Cyber Crime.
- All local authorities in England publish spend and contract data.
- *"Cyber security is the latest name for something we've been doing for quite some time, and that's* ***information assurance*** *(IA). IA is 80% of 'cyber' and that's defensive aspects. Then there are offensive aspects of cyber, which you can put down to penetration testing, IT health checks, monitoring networks, et cetera. And that's responding, really, to the new threat. Terrorists. Money laundering. Criminality. Intellectual property theft. It's a very complex environment"* (de Silva, 2011a).
- ***IA*** *is a topic that is becoming integral to US national security. We can no longer rely solely on our armed forces to defend the nation. Professionals in the commercial and government sectors must do their part to defend our critical information infrastructures from cyberattacks* (de Silva, 2011b).
- *…it's about* ***assurance*** *that you have done what you said you would do, to achieve a risk posture that suits the needs of the organisation.* Donn Parker, 30 Aug 2011, per comms.
- *By 2015, the aspiration is that the measures outlined in this strategy will mean the UK is in a position where: law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective* ***cyber security*** *is seen as a positive for UK business; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to our national infrastructure and national security have been confronted* (UK Cabinet Office, 2011e).

12.5.377 **January 2011** - All local authorities in England were required to publish spend and contract data.

12.5.378 **January 2011** - *OECD/IFP Project on "Future Global Shocks" "Reducing Systemic Cybersecurity Risk"* (OECD, 2011) This has been a widely received and referenced report. There is an interesting concept referenced within – that of an "IA engineering framework. … Counter-Measures need to be considered within an IA engineering framework, in which preventative and detective technologies are deployed alongside human-centred managerial policies and controls". The report provides useful historical chronology pointing to how the rhetoric arrived at the "cyber" label:

> Towards the end of the 1990s, analysts began to use the phrase information assurance. This is an altogether softer form of analysis, which recognises that in the absence of solid risk data it is better to identify all the elements that make it more or less likely that there will be a security breach. The approach retains many elements of risk analysis and does not altogether dismiss the virtues of security standards, but it also seeks to borrow ideas from the social sciences: management science to understand how organisations work and how security considerations operate within them; anthropology and criminology to identify how individuals and groups behave and are motivated; psychology to develop an understanding of — people factors in the design of ICT and security; and economics to understand how organisations make security decisions (Backhouse and Dhillon, 2000, p.34).

12.5.379 **January 2011** – *Supplier IA Assessment Framework and Guidance* (UK CESG, 2011) This is an interesting document providing IRM guidance and question sets and tool specifications that can be used

by suppliers of key business services to HMG. The aim of the tool is to provide assurance that HMG's requirements for effective IRM are managed by ICT suppliers and within their own supply chains. This is one of a range of government produced documents that uses a number of different terms that could leave the reader confused. In particular, in the question set, there is reference, in one section alone to *data assurance (security), IRM and IA*. There is a reference to definitions to be used in "Annex A, AS6" but no routing through to this so the reader is left, if reading in the abstract, none the wiser as to the intended meaning of the multitude of terms used.

12.5.380 **January 2011** – *UK Census Security: Report of the Independent Review Team* This report is a measured and helpful account of the state of security and measurement against the IA Maturity Model (IAMM) of the UK Census 2011. This report also provides a helpful statement of the alignment between assurance and security as referenced in paragraph 3.1.22 (Dowdall, Mattinson and Fagan, 2011).

12.5.381 **February 2011** – *IAAC Work Programme 2012* – agreed by the IAAC Board, to include the Three year Business Plan for 2011 to 2013, with a focus on *Consumerisation* and IA issues in shared services in the Cloud. More specifically, this led to a study of *IA and Consumers: Understanding the Sea Change in the Use of Information (The Relevance of IA in the context of Consumerisation)*. The programme included close liaison with academia.

12.5.382 **February 2011** – *Data Centre Strategy, G-cloud and Government Applications Store, Programme Phase 2, Scope Report.* Whilst referencing IA a number of times, the outcome is not clear. "Given that significant value comes from up front, sharable work on commercials, service management and IA, frameworks will be developed in each of these areas to enable certification/validation on a component level, so that work does not have to be repeated when components are assembled into new combinations". This implies yet more IA frameworks will be developed in spite of this Research showing the volume of available material and that there is little justification for spending yet more tax payers money on building more wheels that will be neither referred to nor used in any meaningful way (UK Cabinet Office, 2011a).

12.5.383 **February 2011** – *PSN Technical Transition Guidance,* Version No. 0.8, prepared February 2011 (UK Cabinet Office, 2011b) – this was a draft document that needed tidying up but given that it was designed to assist those in the public sector seeking to transition systems containing large volumes of public personal data across from one secure network to another, the lack of explicitly reference to IA requirements in a meaningful way, together with an absence of a workable checklist, made it quite a wordy document that was not necessarily likely to be of active use to any reader.

12.5.384 **March 2011** – *UK Government ICT Strategy* (UK Cabinet Office, 2011c and Glyck, 2011) – the Strategy contains only one mention of IA and no specific pick up on the action for how to follow through on this, so it is not clear how this is as joined up as the rhetoric around its launch would have one believe. Francis Maude said of the strategy that it is "lapidary" – that is a polishing of something to make it new, to you and me." (Hall, 2011b) This strategy has been described as including a "commitment to accountability", but this should not be something new to be lauded as it should have been embedded as a "must" from the outset. There is a claim of "a definition of mandated standards" that has not been seen before which is welcome news in raising the importance level.

12.5.385 **March 2011** – *CESG Certification for IA Professionals* – first version of the intended certification scheme documentation identifying roles and skill levels issued. Revised in September 2012 and again in February 2015. The scheme is operated by IISP, BCS and APMG.

12.5.386 **June 2011** – *Preparing the local public sector for risk governance: First steps towards an ISO31000 framework* **–** this was a report output from a roundtable conducted by Marsh on public risk governance and it sets the "tone at the top" with regard to embedding a risk culture across all organisations. It provides a helpful list of strategic risks to be considered and a good visual representation of risk control mechanisms and should be seen as a useful addition to the learning portfolio for anyone charged with risk management in their organisation.

12.5.387 **November 2011** – *US Blueprint for a Secure Cyber Future* **–** detailing Cybersecurity Strategy for the Homeland Security Enterprise, highlighting the scale of the cyberspace threat and confirming that addressing cybersecurity is a shared responsibility.

12.5.388 **November 2011** – ***UK Cyber Security Strategy*** (UK Cabinet Office, 2011d) – set out how the government planned to deliver the National Cyber Security Programme through to 2015, with funding of £650 million.

12.5.389 **December 2011** – HMG launched ***Information Principles*** detailing 7 key information principles which have significant implications:

1) Information is a valued asset
2) Information is Managed
3) Information is Fit for Purpose
4) Information is Standardised and Linkable
5) Information is Re-used
6) Public Information is Published
7) Citizens and Businesses can access information about themselves

2012 Highlights / Lowlights

- Australian parliament passed a Cybercrime Legislation Amendment Bill
- Wikileaks biggest media impact - https://wikileaks.org/
- The rise of 3D printing

12.5.390 **31 January 2012** – ***UK Cyber Security Strategy***, *Record of a Joint Cabinet Office/IAAC Seminar* – identified four key outcomes that required collective support and effort between the public sector, the private sector and academia:

1) To define the educational training needs from pre-school to post graduate level
2) To develop an effective approach to communicating the issues of cyber security across the domains of large organisations, SMEs and to the public at large
3) To define and implement an effective career development approach for government and industry in order to promote the engagement with new talent and achieve a high level of professionalism
4) To develop an imaginative approach to incentivise young people to engage and contribute to the OCSIA/IAAC programme

12.5.391 **March 2012** – *InfoSec Assurance Capability Maturity Model (ISA-CMM)*, issued by Carnegie Mellon (Carnegie Mellon, 2012) to support the *US National Strategy to Secure Cyberspace* (US DHS, 2003). A System Security Engineering Capability Maturity Model had been in existence in one form or another since 1995. There was also an international standard built in this area - ISO/IEC 21827:2008. This latest iteration saw a combination of both terms to create a new definition:

> InfoSec Assurance is the assurance level that can be associated with the security that the system (e.g., technical, procedural, etc) uses to protect the information. Since it is impractical for security to guarantee that information is totally protected from exploitation, there is a level of assurance that is associated with the ability of the system to protect the information. InfoSec Assurance services analyse this level of InfoSec Assurance through analysis of information criticality, vulnerability, threat, impact, risk, and countermeasures. Although InfoSec Assurance services can be performed on developmental as well as operational systems, the focus of this current version of the ISA-CMM is the analysis of operational systems.

12.5.392 **6 September 2012** – CESG, Cabinet Office and CPNI jointly launched *Cyber Security Guidance for Business* (UK CESG, 2012a)– consisting of three products:

12.5.392.1 Aimed at senior executives, this offered some high level questions which we believe will assist and support them to determine their critical information assets, support them in their strategic level risk discussions and help them ensure that they have the right safeguards and cultures in place.

12.5.392.2 An Executive Companion which discussed how Cyber Security is one of the biggest challenges that business and the wider UK economy face today. It offered guidance for business on how together we can make the UK's networks more resilient and protect key information assets against cyber threats. The document focused around key points of risk management and corporate governance and includes some anonymous case studies based in real events.

12.5.392.3 The third product supports the Executive Companion and provides more detailed cyber security information and advice for 10 critical areas (covering both technical and process/cultural areas). If implemented as a set it can substantially reduce the cyber risk by helping to prevent or deter the majority of types of attacks.

The material integrates the "Top 20 Critical Controls for Effective Cyber Defence" as endorsed by CPNI (2012). These controls provide further detailed guidance.

12.5.393 **September 2012** – HMG launched ***'10 Steps to Cyber Security'*** . (UK GCHQ, 2015) – guidance to encourage organisations to consider whether they were managing their cyber risks:

1) IRM Regime
2) Secure configuration
3) Network protection
4) Managing user privileges
5) User education and awareness
6) Incident management
7) Malware protection
8) Monitoring
9) Removable media controls
10) Home and mobile working

2013 Highlights / Lowlights

- Early June 2013 saw the release (leaking) of classified NSA documents from to journalists worldwide by **Edward Snowden** – a former government contractor. This set a change of direction as the progress that was being made up to that point, embedding IA into the culture and thinking, was taken off course, as a result of this distraction.
- The rise of **Big Data**.
- December 2013 – **110 million** people affected by a breach at **Target**.

12.5.394 **February 2013** – ***The UK Cyber Security Strategy: landscape review*** – carried out by the National Audit Office (NAO), identified six key challenges facing the government in succeeding on delivering the strategy as described:

- *the need to influence industry to protect and promote itself and UK plc;*
- *to address the UK's current and future ICT and cyber security skills gap;*
- *to increase awareness so that people are not the weakest link;*
- *to tackle cybercrime and enforce the law;*
- *to get government to be more agile and joined-up; and*
- *to demonstrate value for money.*

12.5.395 **February 2013 – *The Global Cyber Game* – an extensive report produced by the Defence Academy of the United Kingdom** (Tibbs *et al*., 2013). This report, prepared for the UK Government, presented a synthesis of the findings of the idea of the *Global Cyber Game* and Cyber Game board as a framework that could be used for practical thinking about cyber strategy.

12.5.396 **February 2013** – *Network InfoSec (NIS) Directive* initially proposed by the European commission to raise cybersecurity capabilities across the EU's 28 member states.

12.5.397 **July 2013** – NIST launches a **Preliminary Framework to Reduce Cyber Risks to Critical Infrastructure**. It was hailed as a way for executives, managers, and staff to: understand and assess the cybersecurity capabilities, readiness, and risks of their organisation and identify areas of strength and weakness and aspects of cybersecurity on which they should productively focus, and learn what informative standards, guidelines, and practices are available and applicable to their organisation. However, given the ongoing cyber breaches, there is an implied lack of adoption of these available frameworks.

12.5.398 **October 2013** – *Government Security Classifications* (UK Cabinet Office, 2013a) - updated, came into force on 2 April 2014.

12.5.399 **September 2013** - *ISF Standard of Good Practice Executive Summary* (ISF, 2013). The definitive guide to enable InfoSec compliance. This is a practical source of InfoSec and information risk-related guidance available. It covers the complete spectrum of InfoSec arrangements that need to be made to keep the business risks associated with IS within acceptable limits, and presents good practice in practical, clear statements. Updates to the *2011 Standard of Good Practice* included reference to the following:

- *Cyber Resilience*
- *Data Analytics*
- *Securing the Supply Chain*
- *BYOD Management Risk*
- *Data Privacy in the Cloud*
- *SANS Top 20 Critical Security Controls*
- *Australian Government Defence Signals Directorate Strategies to Mitigate Targeted Cyber Intrusions*
- *UK Government's (CESG) 10 Steps to Cyber Security*
- *PAS 555*

12.5.400 **November 2013** – ***Cyber governance health check: 2013*** (UK Cabinet Office, 2013b). This review identified that 58 per cent of companies have assessed themselves using an online tracker tool against the 10 Steps guidance since it was first launched. This was up from 40 per cent in 2012. An Executive Companion publication was also produced.

12.5.401 **December 2013 – Cyber Primer** (UK MoD, 2013) – introduces "cyber" in the defence context. Cyber and cyberspace are articulated fully. This publication was shared widely across UK Government departments.

2014 Highlights / Lowlights

A year of breach / loss – a full report is available here:
http://www.idtheftcenter.org/images/breach/DataBreachReports_2014.pdf

This website provides a chronology of the numbers of people affected by breaches:
http://www.bankinfosecurity.co.uk/infographic-2014s-top-breaches-so-far-a-7408#

Amongst the biggest numbers that stand out are the following:

- 76 million household customers and 7 million business customers affected by a lack of protection of two-factor authentication leading to a breach at JPMorgan Chase.
- 53 million customers email addresses compromised with the theft of a third party vendor's user credentials from the Home Depot.
- 4.5 million patients affected by a breach at The Community Health Systems in the US when attackers exploited the infamous Heartbleed vulnerability.
- Mid-2014 – "security experts reported that a gang called CyberVor ('vor' is Russian for 'thief') had stolen 1.2 billion unique credentials" – if validated, this would be the biggest (known) single crime in terms of people affected (Lucas, 2015, p.11).

12.5.402 **April 2014 – *HMG Security Policy Framework*** (UK Cabinet Office, 2009f)– re-released and addressed

- *Good Governance*
- *Culture and Awareness*
- *Risk Management*
- *Information*
- *Technology and Services*
- *Personnel Security*
- *Physical Security*
- *Incident Management*

12.5.403 **June 2014** – ***Cyber Essentials* launched** (UK HMG, 2014) as a result of a call for evidence during 2013 – to coalesce the views of multiple players – and narrowed the landscape still further to five (5) areas of focus:

1) secure configuration basics;
2) boundary firewalls and internet gateways;
3) access control and administrative privileges;
4) patch management; and
5) malware protection basics.

There are two levels – ***Cyber Essentials***, which is a self-assessment online questionnaire for internal completion and signature by a board member and ***Cyber Essentials Plus*** – where tests are carried out by an external body for validation and certification purposes.

12.5.404 **Late 2014** – Microsoft's ***Trustworthy Computing Initiative*** was closed and staff were redistributed.

12.5.405 **December 2014** – *The Internet of Things: making the most of the Second Digital Revolution (UK Government Office for Science, 2014. p.8)* – a paper commissioned by the UK Prime Minister into the Internet of Things and its likely impact, written by the UK's Chief Scientific Advisor, Mark Walport. Walport highlighted that for the system connectivity to work safely and effectively, all data and devices must have proportionate "security by default". "Standards must protect against cybercrime and national security threats, and help to ensure that the system is trustworthy and trusted". Walport acknowledged that as the UK is part of a global economy it would be impossible to set a global standard. However, he recommended that the Government "should take a proactive role in driving harmonisation of standards internationally". CPNI and CESG were recommended to work with industry and international partners to agree best practice security and privacy principles based on "security by default".

2015 Highlights / Lowlights

- 21 million records taken from the US Office of Personnel Management, possibly by China.
- 4,000 records, some with "sensitive" information, stolen from the Joint Chiefs civilian email system, possibly by Russia.
- 32 million records taken from the "cheating" site, Ashley Maddison.
- Schrems wins Privacy case against Facebook (Cordery, 2015).
- **487,731,758** leaked records, including TalkTalk. 80% of companies had a security incident in 2015 (ISM, 2015).
- Over 200 billion emails sent every day; 2.5 billion people sending them (Lucas, 2015, p.xviii).

12.5.406 **January 2015** – ***10 Steps to Cyber Security*** re-launched (UK GCHQ, 2015) - updated to ensure continuing relevance. Covering ten areas of known best practice not dissimilar to the 20 SANS Critical Controls / Cyber Controls:

1) IRM Regime
2) Secure configuration
3) Network Security
4) Managing user privileges
5) User education and awareness
6) Incident management
7) Malware prevention
8) Monitoring
9) Removable media controls
10) Home and mobile working

12.5.407 **January 2015** – *CESG IA Assurance Landscape Survey* – headlined as such, however, immediately goes on to query cyber security measures in place:

> CESG are undertaking a study to ensure you have access to the right 'assurance activities' - things which give you confidence that you have the right level of cyber security in-place. We would welcome your support in this by indicating in the grid below how you manage cyber risk in your own organisation. For ease we have based the grid on the "10 Steps" with which you should be familiar. Your answers will be treated in complete confidence and only used to help us understand the effectiveness of our existing approaches and any gaps.

12.5.408 **29 May 2015** – *NHS Information Governance Toolkit* (UK NHS, 2015) – the 13th version was launched, with requirements addressing significant changes, responding to the Caldicott 2 report as well as changes in the NHS England Standard contract. The updates also include the removal of references to deprecated standards, guidance, knowledge base, publications etc. The Toolkit includes an Incident Reporting Tool for Reporting, Managing and Investigating IG and Cyber Security Serious Incidents Requiring Investigation.

12.5.409 **June 2015** – *A Question of Trust: Report of the Investigatory Powers Review* (Anderson, 2015) – a well-received report by David Anderson, Independent Reviewer of Terrorism Legislation. This extensive paper influenced the planned changes to the Data Retention and Investigatory Powers Act (DRIPA) 2014, and examined:

- The threats to the United Kingdom
- The capabilities required to combat those threats
- The safeguards to protect privacy
- The challenges of changing technologies, and
- Issues relating to transparency and oversight.

12.5.410 **July 2015** – *Cybersecurity Principles and Learning Outcomes for Computer Science and IT-Related Degrees: A resource for course designers and accreditors*, Version 1.1, July 2015 – updating the 2013 first edition. The Principles seek to ensure that content will be integral to computing course and not just a module added on. However, equally the concerns are beyond that of the computing sector specifically – they are *business* issues. ((ISC)², 2015g)

12.5.411 **September 2015** –*G20/OECD Principles of Corporate Governance,* (OECD, 2015) OECD Report to G20 Finance Ministers and Central Bank Governors, September 2015 – six principles core to financial markets management. The report identifies that there is no single model for corporate governance – although most models have common elements.

12.5.412 **6 October 2015** – European Court of Justice (EUCJ) declared previous acceptance of US Safe Harbor Privacy Principles invalid. This reversed a fifteen-year policy of allowing data governed by Directive 95/46/ES to be stored in the US despite the lack of national data protection law.

12.5.413 **December 2015** – *General Data Protection Regulation (GDPR)* put forth by the European Commission in 2012, finally agreed upon by the European Parliament and Council, set to replace the Data Protection Directive 95/46/ec. Approved **14 April 2016**.

12.5.414 **December 2015** - *Network InfoSec (NIS) Directive* – the European Council reach an informal agreement with the Parliament on 7 December and the agreed text was approved by the Member States on 18 December. Awaiting "technical finalisation" at the time of thesis completion; expected Spring 2016. Member States will then have 21 months to implement the Directive into law.

12.5.415 **October 2016** – *National Cyber Security Centre* – NCSC – opened in London, with 700 staff tasked with bolstering security against the growing online threats from around the globe. The NCSC, believed to be a world first with its links to the intelligence service, will have four key objectives (UK HMG, 2016a):

- Understand the cyber security environment, share knowledge and use that expertise to identify and address systemic vulnerabilities
- Reduce risks to the UK by working with public and private sector organisations to improve their cyber security – including the provision of bespoke advice and guidance, help to design and test networks, and exercise response arrangements.
- Respond to cyber security incidents to reduce the harm they cause to the UK - to minimise their damage, help with recovery and learn lessons to reduce the chance of recurrence and minimise future impact. For very serious incidents, messages may have to be issued on how the public can protect themselves.
- To nurture and grow Britain's cyber security capability and provide leadership on critical national cyber security issues, by identifying threats and technology trends.

12.5.416 **3 November 2016** – the next five year *National Cyber Security Strategy 2016 - 2021* was launched, reflecting a £1.9bn package of defence funding designed to improve the UK's cyber security, repeating many of the existing objectives, including the intention to ensure that the UK is the most secure place to do business (UK HMG, 2016b).

12.5.417 **February 2017** – IAAC *Cyber Profession* paper (IAAC, 2017) produced as a result of starting with the Professionalism findings from this research and building upon the work to identify some future recommendations for the profession. This paper introduced the term GRADE A to cover the breadth of possible actors across Governors; Risk Managers; Auditors/Assessors; Defenders (incorporating testers, analysis and operators); Engineers and Architects.

12.5.418 **May 2017** – The UK Government funded an initiative to create a "Cyber security Body of Knowledge (CyBoK).

12.6 Where is IA Going?

12.6.1 The move towards digital storage and extensive dissemination of information created both opportunity and risk:

- ***Opportunity*** *because it has never been easier, given the right management systems, to share information across an organisation and with partners on a distributed, global basis*
- ***Risk*** *because, without adequate technical and procedural controls, unauthorised and inappropriate usage of information has been made much easier.*

12.6.2 The central issue for most organisations is to balance the need to generate the maximum return from the value of the information they possess which, in practice, can only be achieved by providing unfettered access to information to those who have a legitimate need with the risk of the damage that unauthorised use can entail. "IA is essential for the delivery of those Government outcomes that are dependent on realising the benefits of Information and Communications Technology" (UK Cabinet Office, 2007a).

12.6.3 In the early 2000s, the approach to InfoSec was based on conventional network and InfoSec paradigms:

- *Network security: protection from inbound penetrative attacks by unauthorized intruders and viruses by the use of firewalls and virus protection software*
- *Information security: control of access by the use of passwords and other means, providing a simple on/off switch to information (access is either granted or not granted).*

12.6.4 These approaches were proven to have the following limitations:

- *Relatively blunt tools, in that they do not specify different circumstances which might dictate different access rights*
- *They usually say little or nothing about what the individual is permitted to do with the information once accessed*
- *They depend crucially on the ability of an organisation to accurately identify individuals and manage passwords (often a vulnerable area of corporate security)*
- *Critically, they place no technical controls on the information once it has left the secure environment.*

12.6.5 The move to deliver government applications using cloud technology services changed information access, management and security needs, adding to the need to improve IA but also changing the culture to accept these new ways of working.

12.6.6 In 2010, it was anticipated that mobile access to the web would overtake desktop in 2014, data and processing would move to the cloud, web would move towards v3.0, the Semantic Web and by then payments via mobile technology would be well embedded. These expectations have been largely borne out and the pace of change continues unabated.

12.6.7 IA was supposed to be moving more towards the ideas of the content industry – solving the conundrum of maximising consumer access while minimising unauthorised usage (Barlas, 2003). Digital rights elements were to be addressed across two categories:

- *Permissions systems which control the use to which a digital file can be put and*
- *Forensic systems running outside the controlled corporate environment, which detect misuse.*

12.6.8 With the continued movement towards "Raw Data Now" (Berners-Lee, 2010) as part of the UK Government's Open Data (and thus transparency) initiatives to make as much information generated in the public sector as available as possible, the pressure was on public sector organisations to be able to evidence their datasets and further scrutiny will ensue if these prove to be inaccurate. The Audit Commission had already highlighted inadequacies and concerns with regard to Data Quality, a subject they have been publishing and reporting on for some time, producing standards in 2007. The advice, guidance and best practice is already available and needs to be being implemented (Audit Commission, 2010). As a result of the trend towards consumerisation, economically it will not be possible to keep building stronger castles (Cole, 2002). The aim, in line with defence in depth strategies, depicted in Figure 94 below, is to limit the damage and reduce the threat. So the IA strategy for the future needs to be focused on reducing impacts on the basis of solid risk assessment understanding.

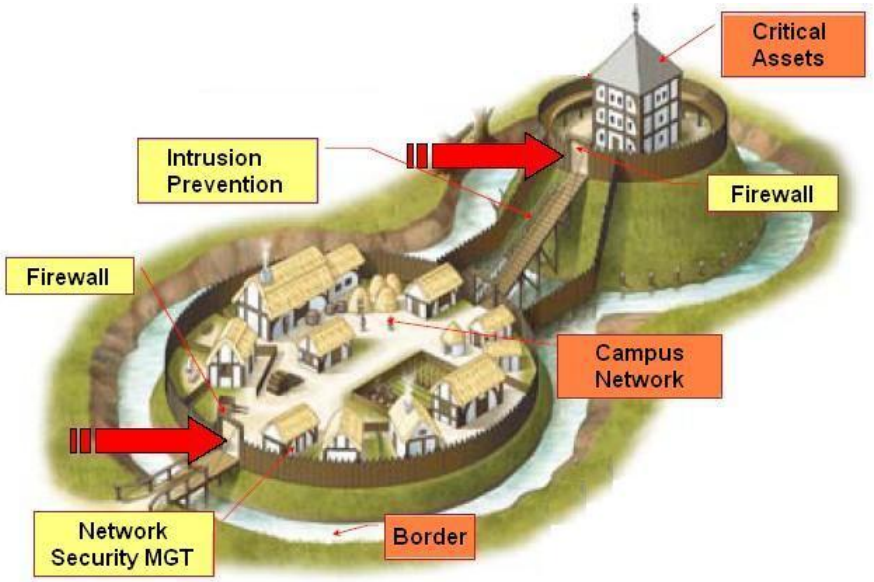


Figure 94: Defence in Depth, Source: Nige the Security Guy (2013)

12.6.9 In 2011, the UK Government pledged to spend £650m during the subsequent four years on a National Cyber Security Programme to protect individuals and the national infrastructure from cyber-attacks (ISM, 2010). However, in March 2016, GCHQ provided commentary advising that despite spending nearly £1 billion on cybersecurity, the expected benefits had not been realised (Gothard, 2016).

12.6.10 The public declaration of data loss incidents will be embraced by the EU GDPR – General Data Protection Regulation. In the main, breaches are already reported to the Information Commissioner at the earliest possible opportunity as, in doing so, the potential penalties are reduced by virtue of early communication and co-operation.

12.6.11 IA is being lost as a term and cybersecurity appears to be winning the day – but in so doing, depth of knowledge is also being lost. This is emblematic of the anti-intellectualism rife in the 21st century and will have future consequences, much of which can be foretold.

> *Information Assurance is actually what is required by us all – in these Internet of Things times, in these interconnected times, mobile payments etc. The need to design in security rather than to leave it as an afterthought is well known amongst the information security community and has been confirmed in recent research from Georgetown University*. (Vaidya, 2015)
>
> *Improving IA is a multifaceted endeavour.* (Ackerman, 2013)

12.7 A Footnote About Risk

12.7.1 The concept of risk is entirely embedded within the thinking of IA practitioners and the available BoK bears this out. A wider review of some key risk papers, as referenced in the Bibliography, attests to issues relating to the difficulty and subjectivity of risk thinking. People do not get "safer" the more they understand and appreciate risk issues – they simply reapportion the risk elsewhere (Shostack and Stewart, 2008, p.97).

12.7.2 Adams' writing on risk management should be compulsory reading as it sets out perspectives of risk assessment in an understandable way that help to better design and assess internal and external risks within a framework of human factors and impacts (Adams, 1999). Recent events provide perspective. For example, "BP had strict guidelines barring employees from carrying a cup of coffee without lid-but no standard procedure for how to conduct a 'negative-pressure test', a critical last step in avoiding a well blow out. If done properly, that test might have saved the Deepwater Horizon" (Fortune, 2011). Unfortunately, there is "no good evidence that training users causes them to behave differently weeks or months after the training" they may have received (Shostack and Stewart, 2008, p.141). Schou and Trimmer (2004) identified, similarly, that "Awareness is at the lowest level of the solution to IA. It is designed

to affect short-term memory. ...One fundamental goal of training programs is motivation of learners to move knowledge and skills from short-term memory into long-term memory. Often, these knowledge and skills are chained sequences of behaviour that require higher level mental processing" (Ibid. p.iv).

12.7.3 There are many ways to view risk. The COSO ERM model provides a different categorisation, shown in the example risk model in Table 31 below:

Environmental Risks	Capital Availability
	Regulatory, Political and Legal
	Financial Markets and Shareholder Relations
	Process Risks
Process Risks	Operations Risk
	Empowerment Risk
	Information Processing / Technology Risk
	Integrity Risk
	Financial Risk
Information for Decision Making	Operational Risk
	Financial Risk
	Strategic Risk

Table 31: Example Risk Model, Source: cited in Bediako (2014), p.30

12.7.4 Fitzgerald (2012) represented the US Federal Information Processing Standard (FIPS 199) System Categorisation showing Potential Impact Definitions for Security Objectives below in Table 32, in such a way as to show the links between the CIA attributes of security and their corresponding risk related impacts.

FIPS 199	**Low**	**Moderate**	**High**
Confidentiality *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]*	The unauthorized disclosure - loss - of **confidentiality** could be expected to have a ***limited adverse effect*** on organisational operations, organisational assets or individuals.	The unauthorized disclosure - loss - of **confidentiality** could be expected to have a ***serious adverse effect*** on organisational operations, organisational assets or individuals.	The unauthorized disclosure - loss - of **confidentiality** could be expected to have a ***severe or catastrophic adverse effect*** on organisational operations, organisational assets or individuals.
Integrity *Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]*	The unauthorized modification or destruction - loss - of **integrity** could be expected to have a ***limited adverse effect*** on organisational operations, organisational assets or individuals.	The unauthorized modification or destruction - loss - of **integrity** could be expected to have a ***serious adverse effect*** on organisational operations, organisational assets or individuals.	The unauthorized modification or destruction - loss - of **integrity** could be expected to have a ***severe or catastrophic adverse effect*** on organisational operations, organisational assets or individuals.
Availability *Ensuring timely and reliable access to and use of information [44 U.S.C., SEC. 3542]*	The disruption of access to or use of information or an information system – i.e. loss of **availability** could be expected to have a ***limited adverse effect*** on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system – i.e. loss of **availability** could be expected to have a ***serious adverse effect*** on organisational operations, organisational assets or individuals.	The disruption of access to or use of information or an information system – i.e. loss of **availability** could be expected to have a ***severe or catastrophic adverse effect*** on organisational operations, organisational assets or individuals.

Table 32: Standards for Security Categorization of Federal Information and IS, Source: NIST (2004a), cited in Fitzgerald (2012), p.126

12.7.5 Whilst acknowledging that "Good risk governance processes can help us avoid very costly or even deadly fates", it appears there is a gap in understanding how vital this information view is in avoiding costly risks being realised (Koenig, 2012, p.185). Table 33 below provides a different set of risk descriptions, than the list in Table 31.

Type	*Definition*
Market Risk	Changes in exchange rates, interest rates, stock prices, carbon prices and other market-priced variables
Credit Risk	Exposure to the failure of a counterparty to a transaction or loan
Operational Risk	The risk of loss resulting from inadequate or failed internal processes, people and systems
Technology Risk	Failure of a technological agent in a system or inadequacy of technology
Reputation Risk	The loss of the value of a brand or ability of an organisation to persuade.
Legal Risk	Changes in regulation, failure to comply with existing regulations, errors in legal agreements, or litigious actions against an organisation
Security Risk	Employee safety, executive protection services, barriers to access of company infrastructure
Liquidity Risk	Loss of short-term financing to facilitate the daily transactions of the organisation, or unexpected demands for funds that cannot be met in a timely fashion
Project Risk	Delays or disruption to the scheduled implementation of key projects.
Supply Chain Risk	Exposure to other agents in our network upon which we rely to supply goods or services that are part of our organisation process or the delivery of our goods or services.
Insurance Risk	The management of risk transfer contracts with various insurance and re-insurance companies, or the failure to obtain appropriate coverage
Environmental Risk	The potential impact of our organisation's activities on its environment or changes in the environment in which we operate that affect our ability to pursue corporate values
Business Continuity Risk	Disruption of our organisation's ability to operate at its normal place or using its normal technologies due to natural or other factors.
Strategic Risk	Misalignment of corporate goals with network member needs or innovation external to the system that replaces or acts as a substitute for an organisation's goods or services.
Enterprise Risk	Integration of all moving parts in the organisation for maximisation of value based on risk-taking capacity.

Table 33: Risk Definitions, Source: Koenig (2012), p.160

12.7.6 Whilst positively, there is mention of "security risk", there is no mention of **Information Risk**, nothing relating to information loss nor corruption and yet in the subsequent two years, data breaches increased exponentially. Perhaps it is intended implicitly. There is mention in the book of the Professional Risk Managers' International Association (PRMIA) (Koenig, 2012, p.113) and the fact that professional risk managers have only come to occupy important roles in their organisations since the mid-1990s and the science of risk management has advanced greatly over that period (Ibid. p.159).

12.7.7 There is much work to be done between the IA professionals and the Internal Audit professionals to ensure that the two directions of business risk consideration meet in the middle and adequately address the needs of the business(es) being served. IA professionals need to be able to share identified business risks with Internal Audit colleagues in advance of them being realised and in advance of them being raised to the Board.

12.7.8 By 2013, the Institute of Internal Auditors had introduced the concept of the "Three Lines of Defense" (3LoD), as a mechanism for providing effective risk management, shown in Figure 95 below.

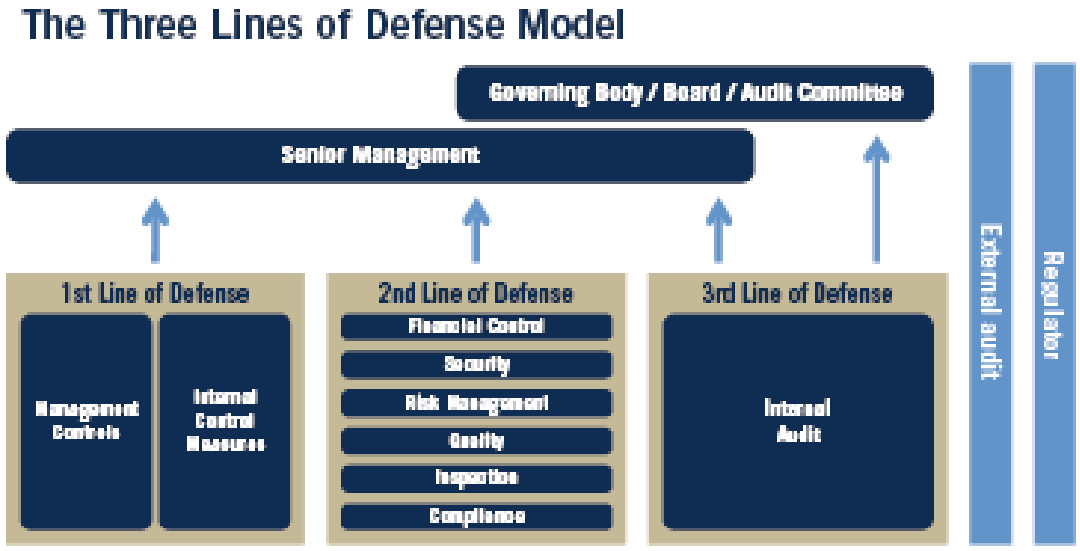


Figure 95: Three Lines of Defense in Effective Risk Management and Control, Source: IIA Position Paper (2013)

12.7.9 Leech (2016) proposed an approach – the Five Lines of Assurance - 5LoA – which more appropriately addresses this maturity, ensuring leadership are positioned as being actively engaged, rather than bystanders, as represented in the flow below in Figure 96.

Figure 96: Five Lines of Assurance, Source: Leech (2016)

12.7.10 However, ensuring evidence of the maturity roadmap, the three lines of defence were updated to reflect nine lines, as shown in Figure 97 below, in the context of a robust enterprise risk management framework.

Figure 97: Stakeholders Lines of Defense, Alleyne *et al* (2016)

12.7.11 There is still a journey to be undertaken to understand the overlay of the importance of the *information lens* in the dialogue. As articulated by McKinsey (2009) "Companies are susceptible to interconnected cascades of risk". Therefore, IA Professionals need a broader perspective to address these cascades.

12.7.12 Information Risk, Reputation Risk, Brand Risk – and the management thereof – are integral parts of corporate governance as much as they are part of IG. Training and education, above and beyond awareness raising, needs to be tailored to address risk perspectives. The resultant trained professionals then need to be empowered to act responsibility in the IA domain and beyond, incorporating all aspects of the "corporate defence umbrella", illustrated in Figure 98 below.

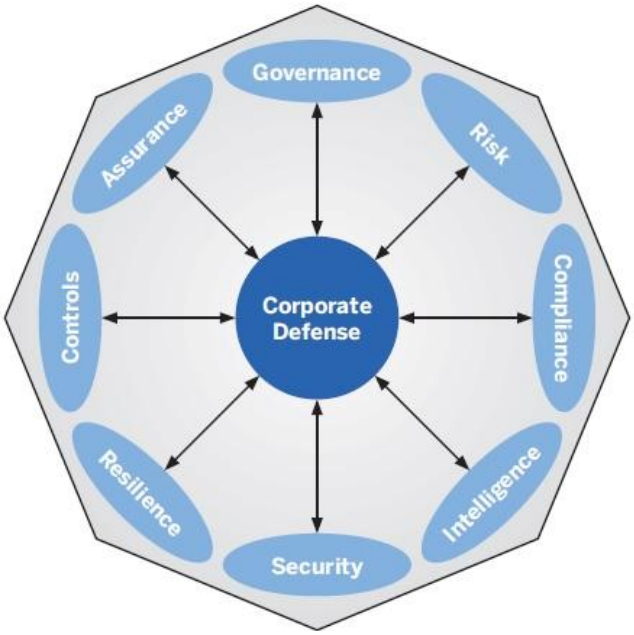


Figure 98: Corporate Defence Umbrella, Source: Lyons (2016)

December 2017